UNIVERSIDADE FEDERAL DO TRIÂNGULO MINEIRO

MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

Divisão de Polinômios Com Duas Variáveis

AIRTON MONTE SERRAT BORIN JUNIOR

Uberaba-MG
2013

Airton Monte Serrat Borin Junior

Divisão de Polinômios com Duas Varáveis

Dissertação de mestrado apresentada ao curso de Mestrado Profissional em Matemática em Rede Nacional-PROFMAT, como parte das atividades para obtenção do título de Mestre em Matemática da Universidade Federal do Triângulo Mineiro - UFTM, Departamento de Matemática.

Uberaba

2013

Catalogação na fonte: Biblioteca da Universidade Federal do Triângulo Mineiro

B739d

Borin Júnior, Airton Monte Serrat
Divisão de polinômios com duas variáveis / Airton Monte Serrat Borin Júnior. -- 2013.
57 f. : il., fig., tab.

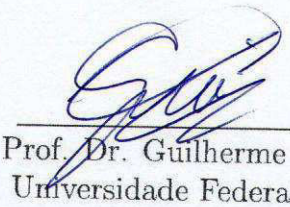
Dissertação (Mestrado Profissional em Matemática em Rede Nacional) -- Universidade Federal do Triângulo Mineiro, Uberaba, MG, 2013.
Orientador: Prof. Dr. Rafael Peixoto

1. Algoritmos-Matemática. 2. Polinômios. 3. Variáveis (Matemática). I. Peixoto, Rafael. II. Universidade Federal do Triângulo Mineiro. III. Título.

Banca Examinadora

Prof. Dr. Rafael Peixoto
Orientador
Unviversidade Federal do Triângulo Mineiro

Prof. Ms. Leonardo Amorim e Silva
Universidade Federal do Triângulo Mineiro



Prof. Dr. Guilherme Chaud Tizziotti
Universidade Federal de Uberlândia

Dedicatória

Dedico a Deus por me dar a cada dia a perseverança e a força para continuar buscando novos conhecimentos e aprendizados e lhe sou grato pelas oportunidades que me deu e continua a dar. Dedico à minha esposa Ana Carolina e ao meu filho Heitor por suportarem a minha ausência devido a várias tarefas acadêmicas e profissionais. Dedico aos meus pais e meus irmãos pelo apoio incondicional em todos os momentos de minha vida. Dedico ao meu orientador, professor Rafael Peixoto pois sem sua atenção, paciência e estímulo este trabalho não teria sido possível. Dedico a todos os professores do Profmat polo Uberaba, por tanto terem me ensinado durante esses dois anos de curso. Dedico aos meus amigos do curso de Mestrado profissional em Matemática que estiveram comigo nesses dois anos de curso e pelas grandes amizades conquistadas neste longo percurso.

Agradecimentos

Ao término deste trabalho, deixo aqui meus sinceros agradecimentos:

– Agradeço ao meu Orientador Prof. Dr. Rafael Peixoto pelos ensinamentos dados

– Agradeço à CAPES pelo fornecimento da bolsa de pesquisa ao longo da Pós Graduação

– Agradeço ao PROFMAT pela oportunidade

– Agradeço aos professores Prof. Ms. Leonardo Amorim e Silva e o Prof. Dr. Guilherme Chaud Tizziotti por terem aceito o convite para fazerem parte da minha banca

Não há ramo da Matemática, por mais abstrato que seja, que não possa um dia vir a ser aplicado aos fenômenos do mundo real. (Lobachevsky)

Resumo

Neste trabalho desenvolvemos um estudo a respeito do algoritmo da divisão de polinômios de duas variáveis. Para isso estudamos os conceitos de divisibilidade e o algoritmo de divisão no conjunto dos inteiros e no anel de polinômios em uma variável. Introduzimos o conceito de ordem monomial e descrevemos o algoritmo de divisão para polinômios em duas variáveis, procurando generalizar aspectos da teoria conhecida para polinômios de uma variável.

Palavras-chave: Algoritmos-Matemática, Polinômios, Variáveis (Matemática).

Abstract

In this work a study about the division algorithm for polynomials of two variables. For this study the concepts of divisibility and the division algorithm on the set of integers and the polynomial ring in one variable. We introduced the concept of monomial order and describe the division algorithm for polynomials in two variables, trying to generalize aspects of the theory known for a variable polynomials.

Keywords: Mathematical algorithms, Polynomials, Variables (Mathematics).

INTRODUÇÃO

A necessidade de realizar a operação de divisão vem de longa data na história da humanidade. Durante a Idade do Bronze já havia a necessidade de se fazer uso do conceito de fração. Mais tarde, por volta de 300 a.c., Euclides no livro *Os Elementos* publica o algoritmo para a divisão de números naturais, usado até os tempos atuais. Com o desenvolvimento da álgebra, surge por volta do século XVI o conceito de polinômio, bem como a divisão de polinômios em uma variável, cujo algoritmo é parecido com o algoritmo da divisão para números inteiros. Em 1965, Bruno Buchberger, em sua tese de Doutorado publica a Teoria das bases de Gröbner para anéis de polinômios, onde apresenta o algoritmo da divisão de polinômios em várias variáveis.

Este trabalho trata do estudo do algoritmo da divisão de polinômios de duas variáveis. Para esse estudo vamos utilizar o conceito de divisibilidade e ordem monomial.

O trabalho está dividido em três capítulos, sendo que no primeiro traremos a definição de divisibilidade nos números inteiros e estudaremos algumas de suas propriedades. Daremos também o algoritmo para a divisão e o algoritmo de Euclides para o cálculo de mdc de números inteiros.

No segundo capítulo, definiremos Anel, Corpo, também definiremos grau e termo líder de polinômios em $K[x]$. Daremos também o algoritmo da divisão e o algoritmo para se determinar o máximo divisor comum de polinômios em $K[x]$.

No último capítulo será apresentado o conceito de ordem monomial para polinômios em $K[x_1, \ ..., \ x_n]$, aqui também estenderemos o algoritmo da divisão de polinômios em $K[x]$ para polinômios em $K[x, y]$ bem como faremos alguns exemplos de divisão de polinômios em $K[x, y]$ com diferentes ordens monomiais.

O primeiro capítulo está baseado em resultados de [1] e [9], o segundo em resultados encontrados em [2], [3] e [7], e o último capítulo foi baseado em [6], [7] e [8]. [4], [5] e [8] foram usados nessa introdução.

Sumário

1 Divisão nos Inteiros

Neste capítulo discorreremos sobre a divisão nos números inteiros como é ensinado no Ensino Básico, bem como algumas de suas propriedades, os conceitos de mdc e mmc, o algoritmo de Euclides para o cálculo do mdc de dois números inteiros e ainda enunciaremos o teorema fundamental da aritmética.

1.1 Divisibilidade

Dados dois números inteiros a e b com $a \neq 0$, diremos que a divide b, escrevendo $a|b$, quando existir $c \in \mathbb{Z}$ tal que $b = a \cdot c$. Neste caso, diremos também que a é um *divisor* ou um *fator* de b ou, ainda, que b é um *múltiplo* de a.

A notação $a|b$ não representa nenhuma operação em $\mathbb{Z}$, tão pouco representa uma fração. Trata-se de uma sentença que diz ser verdade que existe c tal que $b = a \cdot c$. A negação dessa sentença é representada por $a \nmid b$, significando que não existe nenhum número inteiro c tal que $b = a \cdot c$.

Exemplo 1.1. $1|0$, $-1|7$, $-2|0$, $2|8$, $5 \nmid 6$, $-8 \nmid 6$.

Suponha que $a|b$ e seja $c \in \mathbb{Z}$ tal que $b = a \cdot c$. O número inteiro c é chamado de *quociente* de b por a e denotado por $\frac{b}{a} = c$ ou por b/a.

Exemplo 1.2. Por exemplo,

$$\frac{6}{3} = 2, \ pois \ 6 = 3 \cdot 2$$

Teorema 1.3. *A divisibilidade tem as seguintes propriedades:*

i. $a|a$

ii. $b|c \Rightarrow ab|ac$

iii. $a \cdot b|a \cdot c \ e \ a \neq 0 \Rightarrow b|c$

iv. $1|a$

v. $a|0$

vi. $a|b \ e \ b \neq 0 \Rightarrow |a| \leq |b|$

vii. $a|b \ e \ b|a \Rightarrow |a| = |b|$

viii. $a|b \ e \ b \neq 0 \Rightarrow (\frac{b}{a})|b.$

Dem. (i.) e **(iv.)** Como $a = 1 \cdot a$ segue que $a|a$ e que $1|a$, inclusive para $a = 0$. **(ii.)** Se $b|c$ então $c = q \cdot b$ para algum inteiro q. Logo $a \cdot c = q \cdot a \cdot b$, assim provamos que $a \cdot b|a \cdot c$. **(iii.)** Se $a \cdot b|a \cdot c$ então $a \cdot c = a \cdot b \cdot q$ para algum inteiro q. Logo $c = q \cdot b$, portanto $b|c$. **(v.)** Como $0 = a \cdot 0$ segue que $a|0$. **(vi.)** Se $a|b$ e $b \neq 0$, existe $c \in \mathbb{Z}$ tal que $b = a \cdot c$. Como $|c| \geq 1$, segue-se que $|a| \leq |a \cdot c| = |b|$. **(vii.)** Se $a|b$ e $b|a$ então existem inteiros não nulos k e q tais que $a = k \cdot b$ e $b = q \cdot a$. Assim $k \cdot q = 1$, logo $|k| = |q| = 1 \Longrightarrow |a| = |b|$.

Vamos demonstrar agora o item **(viii.)**. Se $a|b$ então $b = c \cdot a$, para algum inteiro c, então $\frac{b}{a}$ é um inteiro. Como $\frac{b}{a} \cdot a = b$ segue que $\frac{b}{a}|b$

■

Proposição 1.4. *Considere a e $b \in \mathbb{Z}^*$ e $c \in \mathbb{Z}$. Temos que se $a|b$ e $b|c$, então $a|c$.*

Dem. De fato, pois se $a|b$ e $b|c$ implica que existem f, $g \in \mathbb{Z}$, tais que $b = a \cdot f$ e $c = b \cdot g$. Substituindo o valor de b, obtido da primeira equação, na segunda equação, obtemos

$$c = b \cdot g = (a \cdot f) \cdot g = a \cdot (f \cdot g),$$

o que nos mostra que $a|c$.

■

Proposição 1.5. *Se a, b, c e $d \in \mathbb{Z}$, com $a \neq 0$ e $c \neq 0$, então $a|b$ e $c|d$ implica que $a \cdot c|b \cdot d$.*

Dem. Se $a|b$ e $c|d$, então existem f, $g \in \mathbb{Z}$, tais que $b = a \cdot f$ e $d = c \cdot g$. Portanto, $b \cdot d = (a \cdot f) \cdot (c \cdot g)$, logo $a \cdot c|b \cdot d$.

■

Exemplo 1.6. Sejam a, b, e $c \in \mathbb{Z}$ e $c \neq 0$, então $a \cdot c|b \cdot c$ se, e somente se $a|b$.

Dem. Pelo Teorema 1.3 item **(iii.)** se $a \cdot c|b \cdot c$ implica que $a|b$. Por outro lado se $a|b$ e $c|c$, pela Proposição 1.5, $a \cdot c|b \cdot c$.

■

Proposição 1.7. *Considere a, b e $c \in \mathbb{Z}$ com $a \neq 0$, tais que $a|\,(b \pm c)$. Então $a|b$ se, e somente se $a|c$.*

Dem. Se $a|(b \pm c)$, então existe $f \in \mathbb{Z}$ tal que $b \pm c = f \cdot a$. Agora, se $a|b$, temos que existe $g \in \mathbb{Z}$ tal que $b = a \cdot g$. Juntando as duas igualdades acima, temos que

$$a \cdot g \pm c = f \cdot a,$$

Da igualdade acima, obtemos

$$c = a \cdot f \mp a \cdot g = a \cdot (f \mp g),$$

o que implica que $a|c$. A volta é análoga.

■

Proposição 1.8. *Se a, b, c e $d \in \mathbb{Z}$, com $a \neq 0$, e x, $y \in \mathbb{Z}$ são tais que $a|b$ e $a|c$, então $a|\,(x \cdot b + y \cdot c)$ e $a|\,(x \cdot b - y \cdot c)$.*

Dem. $a|b$ e $a|c$ implicam que existem f, $g \in \mathbb{Z}$ tais que $b = a \cdot f$ e $c = a \cdot g$. Logo, $x \cdot b \pm y \cdot c = x \cdot (a \cdot f) \pm y \cdot (a \cdot g) = a \cdot (x \cdot f \pm y \cdot g)$, o que prova o resultado.

■

Exemplo 1.9. Como $3|15$ e $3|42$, então $3|(8 \cdot 15 - 7 \cdot 42)$.

1.2 O Algoritmo da Divisão de Euclides

Antes de enunciarmos o Algoritmo da Divisão para os números inteiros, vamos enunciar o algoritmo da divisão para os números naturais feita por Euclides e o Teorema de Eudoxius.

Teorema 1.10 (Divisão Euclidiana). *Sejam a e b dois números naturais com $0 < a < b$. Existem dois únicos números naturais q e r tais que*

$$b = a \cdot q + r, \ \textit{com } r < a.$$

Dem. Sejam a e b números naturais tais que $b > a$ e considere, enquanto fizer sentido nos naturais, os números

$$b, b - a, b - 2a, ..., b - n \cdot a, ..$$

Pela *Propriedade da Boa Ordem* [1], o conjunto S formado pelos elementos acima tem um menor elemento $r = b - q \cdot a$. Vamos provar que r tem a propriedade requerida, ou seja, que $r < a$.

Se $a|b$, então $r = 0$, a demonstração está concluída. Se, por outro lado, $a \nmid b$, então $r \neq a$, e, portanto, basta mostrar que não pode ocorrer $r > a$. De fato, se isto ocorresse, existiria um número natural $0 < c < r$ tal que $r = c + a$. Consequentemente, sendo $r = c + a = b - q \cdot a$, teríamos

$$c = b - (q + 1) \cdot a \in S, \ com \ c < r$$

contradição com o fato de r ser o menor elemento de S.

Portanto, temos que $b = a \cdot q + r$ com $r < a$, o que prova a existência de q e r.

Agora, vamos provar a unicidade. Note que, dados dois elementos distintos de S, a diferença entre o maior e o menor desses elementos, sendo um múltiplo de a, é pelo menos a.

Sejam $r = b - a \cdot q$ e $r' = b - a \cdot q'$, com $r < r' < a$, assim $r' - r = b - a \cdot q' - (b - a \cdot q) = a \cdot (q - q')$. Como $q - q' \geq 1$, segue que $r' - r \geq a$ o que implica que $r' \geq r + a \geq a$, absurdo. Portanto, $r = r'$.

Daí segue-se que $b - a \cdot q = b - a \cdot q'$, o que implica que $a \cdot q = a \cdot q'$ e, portanto, $q = q'$.

■

Teorema 1.11 (**Teorema de Eudoxius**). *Dados a e b inteiros com $b \neq 0$ então a é um múltiplo de b ou está entre dois múltiplos consecutivos de b, ou seja, para cada par de números inteiros a e b, com $b \neq 0$, existe um número inteiro q tal que, para $b > 0$,*

$$q \cdot b \leq a < (q + 1)b$$

e para $b < 0$,

$$q \cdot b \leq a < (q - 1)b$$

Dem. Dados a e b inteiros com $b \neq 0$, ou $b|a$ ou $b \nmid a$. No caso em que $b|a$ sabemos que a é um múltiplo de b, por outro lado, no caso em que $b \nmid a$, temos que a não é um múltiplo de b. Então, nós dividimos a demonstração em dois casos. No primeiro caso, considerando-se que a é múltiplo de b, e no outro caso, considerando-se que a não é um múltiplo de b.

[1] Todo subconjunto não vazio do conjunto dos números naturais possui um menor elemento.

i. Suponha a um múltiplo de b. Isso significa que $b|a$, ou seja, que $a = q \cdot b$, para algum inteiro q. Demonstramos assim o primeiro caso do teorema.

ii. Suponha agora que a não é um múltiplo de b. Isso significa que $b \nmid a$. Se $b \nmid a$, então, pela *Propriedade Arquimediana* [2] temos que $a < b \cdot k$, ou seja, a deve ser menor do que um múltiplo de b, para algum k inteiro. E mais, $q \cdot b < a$, ou seja, a deve ser maior que um múltiplo q de b, para algum q inteiro. Então, temos que a está entre dois múltiplos de b. Tomando q como o maior inteiro tal que $q \cdot b < a$ e k o menor inteiro tal que $a < k \cdot b$, temos

$$q \cdot b < a < k \cdot b$$

O que temos que provar agora é que $k = q + 1$ para $b > 0$ e $k = q - 1$ para $b < 0$. Vamos provar para o caso $b > 0$. Supondo, por absurdo que $k > q + 1$, onde q é o maior inteiro tal que $b \cdot q < a$. Sabemos que $q \cdot b < a < b \cdot k$, isso significa que a pode assumir qualquer valor neste intervalo, ou seja, $a = (q + 1) \cdot b$, o que implica que a é um múltiplo de b, o que contradiz a hipótese de a não ser múltiplo de b. Assim, k deve ser igual a $(q + 1)$, portanto $q \cdot b < a < (q + 1) \cdot b$. A demonstração para o caso de $b < 0$ é análoga.

■

Teorema 1.12. *Dados a e b dois números inteiros com $b \neq 0$. Então existem únicos inteiros q e r tais que $a = q \cdot b + r$ e $0 \leq r < |b|$, onde q chama-se o quociente, r o menor resto não-negativo na divisão de a por b.*

Dem.

i. Para $b > 0$, pelo Teorema 1.11, existe q inteiro tal que

$$q \cdot b \leq a < (q + 1) \cdot b$$

subtraindo $q \cdot b$ temos

$$0 \leq a - q \cdot b < (q + 1) \cdot b - q \cdot b = b$$

Se definirmos $r = a - q \cdot b$, então $0 \leq r < |b|$ e $a = q \cdot b + r$.

ii. Para $b < 0$, pelo Teorema 1.11, existe q inteiro tal que

$$q \cdot b \leq a < (q - 1) \cdot b$$

[2] Se p e q são dois números racionais positivos, existe um inteiro positivo n tal que $n \cdot p > q$.

subtraindo $q \cdot b$ temos

$$0 \leq a - q \cdot b < (q-1) \cdot b - q \cdot b = -b$$

Se definirmos $r = a - q \cdot b$, então $0 \leq r < |b|$ e $a = q \cdot b + r$

Assim foi demonstrada a existência do quociente e do resto. Agora vamos demonstrar a unicidade. Para demonstrar a unicidade suponha que há q_1 *e* r_1 tais que

$$a = q_1 \cdot b + r_1 \; com \; 0 \leq r_1 < |b|$$

assim temos que $(q \cdot b + r) - (q_1 \cdot b + r_1) = 0$ então $b \cdot (q - q_1) = (r_1 - r)$ o que implica que $b|(r_1 - r)$. Mas, como $r_1 < |b|$ *e* $r < |b|$, temos que $|r_1 - r| < |b|$ e como $b|(r_1 - r)$ devemos ter $r_1 - r = 0$, logo $r_1 = r$, o que implica que $q \cdot b = q_1 \cdot b \Longrightarrow q = q_1$ uma vez que $b \neq 0$.

■

Exemplo 1.13. O quociente e o resto da divisão de 27 por 11 são $q = 2$ e r = 5. O quociente e o resto da divisão de -27 por 11 são $q = -3$ e $r = 6$.

Exemplo 1.14. Um número natural a é par se, e somente se, a^n é par, qualquer que seja $n \in \mathbb{N}$.

Dem. Seja a um número natural par, então $2|a$, logo existe $q \in \mathbb{N}$ tal que $a = 2 \cdot q$, assim, para um número natural n qualquer $a^n = (2 \cdot q)^n = 2^n \cdot q^n = 2 \cdot 2^{n-1} \cdot q^n = 2 \cdot q'$, $q' \in \mathbb{N}$ e dessa forma $2|a^n$, logo a^n é par. Por outro lado se para um número natural n qualquer, a^n é par, então $a^n = 2 \cdot k$, $k \in \mathbb{N}$. Suponha por absurdo que a não seja par, então existe $q \in \mathbb{N}$ tal que $a = 2 \cdot q + 1$, logo $a^n = (2 \cdot q + 1)^n = (2 \cdot q)^n + n \cdot (2 \cdot q)^{n-1} + ... + \frac{n!}{p! \cdot (n-p)!} \cdot (2 \cdot q)^p \cdot 1^{n-p} + ... + 1^n = 2 \cdot k + 1$, onde $p = 1, 2, 3, ..., n$ e $k = 2^{n-1} \cdot q^n + n \cdot 2^{n-2} \cdot q^{n-1} + ... + n \cdot q$. Dessa forma $2 \nmid a^n$ o que implica que a^n não é par, o que é absurdo. Portanto a é par.

■

1.3 Máximo Divisor Comum e Mínimo Múltiplo Comum

Nessa seção vamos definir *Máximo Divisor Comum* e *Mínimo Múltiplo Comum*.

Definição 1.15. Dados dois números inteiros a e b, não simultaneamente nulos, diremos que o número inteiro $d \in \mathbb{Z}$ é um divisor comum de a e b se $d|a$ e $d|b$.

Definição 1.16. Diremos que um número inteiro d é um máximo divisor comum (mdc) de a e b, não simultaneamente nulos, denotado por (a, b), se possuir as seguintes propriedades:

i. d é um divisor comum de a e de b, e

ii. d é divisível por todo divisor comum de a e b.

A condição **(ii.)** acima pode ser reenunciada como segue:

ii'. Se c é um divisor comum de a e b, então $c|d$.

Portanto, se d é um mdc de a e b e c é um divisor comum desses números, então $|c|$ divide d e, portanto, $c \leq |c| \leq d$. Dessa forma o *máximo divisor comum* de dois números é o maior dentre todos os divisores comuns desses números.

Em particular, isto nos mostra que se d e d' são dois mdc de um mesmo par de números, então , $d \leq d'$ e $d' \leq d$, logo $d = d'$, assim, se existir,o mdc de dois números é único.

Como o mdc de a e b não depende da ordem em que a e b são tomados, temos que

$$(a, b) = (b, a)$$

Proposição 1.17. *Para todo $b \in \mathbb{Z}$, temos que $a|b$ se, e somente se $(a, b) = |a|$:*

Dem. Se $a|b$, então $|a|$ é um divisor comum de a e b, e, se c é um divisor comum de a e b, então c divide $|a|$, o que mostra que $|a| = (a, b)$. Por outro lado, se $(a, b) = |a|$, segue-se que $|a|$ divide b, logo $a|b$.

■

Observe que dados a e $b \in \mathbb{Z}$ não ambos nulos, se existir o mdc (a, b) de a e b, então $(a, b) = (-a, b) = (a, -b) = (a, b)$. Dessa forma, para efeito do cálculo do mdc de dois números, podemos supô-los não negativos.

Agora iremos provar a existência do máximo divisor comum de dois inteiros não negativos, mas para isso vamos utilizar o resultado seguinte, chamado de *Lema de Euclides.*

Lema 1.18 (Lema de Euclides). *Considere $a,\ b$ e $n \in \mathbb{Z}$. Se existe $(a, b - n \cdot a)$, então (a, b) existe e $(a, b) = (a, b - n \cdot a)$:*

Dem. Seja $d = (a, b - n \cdot a)$. Como $d|a$ e $d|\ (b - n \cdot a)$, segue que d divide $b = b - n \cdot a + n \cdot a$. Logo, d é um divisor comum de a e b. Suponha agora que c seja um divisor comum de a e b. Logo, c é um divisor comum de a e $b - n \cdot a$ e, portanto, $c|d$, assim demonstramos que $d = (a, b)$.

■

Algoritmo de Euclides: Daremos agora a demonstração construtiva da existência do mdc dada por Euclides. Tal método é chamado de *Algoritmo de Euclides*.

Dados a, $b \in \mathbb{N}$, podemos supor $a \leq b$. Se $a = 1$ ou $a = b$, ou ainda $a|b$, já vimos que $(a, b) = a$. Suponhamos, então, que $1 < a < b$ e que $a \nmid b$. Logo, pela divisão euclidiana, podemos escrever

$$b = a \cdot q_1 + r_1, \ com\ 0 < r_1 < a.$$

Temos duas possibilidades:

1. $r_1|a$ já, e, em tal caso, pela Proposição 1.17 e pelo Lema 1.18,

$$r_1 = (a, r_1) = (a, b - q_1 \cdot a) = (a, b)$$

   e termina o algoritmo, ou

2. $r_1 \nmid a$, e, em tal caso, podemos efetuar a divisão de a por r_1, obtendo

$$a = r_1 \cdot q_2 + r_2, \ com\ 0 < r_2 < r_1$$

Novamente, temos duas possibilidades:

1. $r_2|r1$, em tal caso, pela Proposição 1.17 e pelo Lema 1.18,

$$r_2 = (r_2, r_1) = (r_1, a - q_2 \cdot r_1) = (r_1, a) = (a, b - q_1 \cdot a) = (a, b)$$

   e termina o algoritmo, ou

2. $r_2 \nmid r_1$, e, em tal caso, podemos efetuar a divisão de r_1 por r_2, obtendo

$$r_1 = r_2 \cdot q_3 + r_3, \ com\ 0 < r_3 < r_2$$

Este procedimento não pode continuar indefinidamente, pois teríamos uma sequência de números naturais $a > r_1 > r_2 > ...$ que não possui menor elemento, o que não é possível pela *Propriedade da Boa Ordem*. Logo, para algum n, temos que $r_n|r_{n-1}$, o que implica que $(a, b) = r_n$.

Exemplo 1.19. Vamos calcular $(56, 21)$ de uma forma prática. Como $56 = 21 \cdot 2 + 14$ vamos posicionar da seguinte forma:

	2	
56	21	
14		

Como $14 \nmid 21$ devemos prosseguir. Dessa forma temos que $21 = 14 \cdot 1 + 7$ e como $7|14$, o processo se encerra e $(56, 21) = 7$.

De forma prática ficaria:

	2	1	2	
56	21	14	7	$\longleftarrow mdc\,(56, 21)$
14	7	0		

Teorema 1.20. *Seja d o máximo divisor comum de a e b, então existem inteiros n e m tais que $d = n \cdot a + m \cdot b$.*

Dem. Considere o conjunto B tal que $B = \{n \cdot a + m \cdot b \backslash n,\ m \in \mathbb{N}\}$. Este conjunto contém, claramente, números negativos, positivos e também o zero. Vamos escolher n e m tais que $c = n \cdot a + m \cdot b$ seja o menor inteiro positivo pertencente ao conjunto B. Vamos provar que $c|a$ e $c|b$. Como as demonstrações são análogas, demostraremos apenas que $c|a$. A prova será dada por contradição. Suponhamos que $c \nmid a$. Neste caso, pelo *Algoritmo de Euclides*, existem q e r tais que $a = q \cdot c + r$ com $0 < r < c$. Portanto $r = a - q \cdot c = a - q \cdot (n \cdot a + m \cdot b) = (1 - q \cdot n) \cdot a + (-q \cdot m) \cdot b$. Isto mostra que $r \in B$, pois $(1 - q \cdot n)$ e $(-q \cdot m)$ são inteiros, o que é uma contradição, uma vez que $0 < r < c$ e c é o menor elemento positivo de B. Logo $c|a$ e de forma análoga se prova que $c|b$.

Como d é um divisor comum de a e b, existem inteiros k_1 e k_2 tais que $a = k_1 \cdot d$ e $b = k_2 \cdot d$ e, portanto, $c = n \cdot a + m \cdot b = n \cdot k_1 \cdot d + m \cdot k_2 \cdot d = d \cdot (n \cdot k_1 + m \cdot k_2)$ o que implica $d|c$. Pelo Teorema 1.3 *(vi)*, temos que $d \leq c$ (ambos são positivos) e como $d < c$ não é possível, uma vez que d é o máximo divisor comum, concluímos que $d = n \cdot a + m \cdot b$.

■

Definição 1.21. Dois números inteiros a e b serão ditos *primos entre si*, ou *coprimos*, se $(a, b) = 1$, ou seja, se o único divisor comum positivo de ambos é 1.

Proposição 1.22. *Dois números inteiros a e b são primos entre si se, e somente se, existem números inteiros n e m tais que $n \cdot a + m \cdot b = 1$.*

Dem. Suponha que a e b são primos entre si. Logo, $(a, b) = 1$. Como, pelo Teorema 1.20, temos que existem números inteiros n e m tais que $n \cdot a + m \cdot b = (a, b) = 1$, segue a primeira parte da proposição.

Reciprocamente, suponha que existam números inteiros n e m tais que $n \cdot a + m \cdot b = 1$. Se $d = (a, b)$, temos que $d|(n \cdot a + m \cdot b)$, o que mostra que $d|1$, e, portanto, $d = 1$.

■

Proposição 1.23. *Se $a|b \cdot c$ e $(a, b) = 1$, então $a|c$.*

Dem. Como $(a, b) = 1$ pela Proposição 1.22 existem inteiros n e m tais que

$$n \cdot a + m \cdot b = 1.$$

Multiplicando-se os dois lados desta igualdade por c temos:

$$n \cdot (a \cdot c) + m \cdot (b \cdot c) = c.$$

Como $a|a \cdot c$ e, por hipótese, $a|b \cdot c$ então, pela Proposição 1.7, $a|c$.

■

Definição 1.24. Um número inteiro n, $n > 1$, possuindo somente dois divisores positivos n e 1 é chamado *primo*. Se $n > 1$ não é primo dizemos que n é *composto*.

Proposição 1.25. *Se $p|a \cdot b$, p primo, então $p|a$ ou $p|b$, a e b inteiros.*

Dem. Seja p um número primo tal que $p|a \cdot b$, onde $a,\ b \in \mathbb{Z}$. Se $p|a$ não há nada a ser demonstrado. Vamos supor então que $p \nmid a$, assim $(a, p) = 1$ o que implica, pela Proposição 1.23, que $p|b$.

■

Teorema 1.26 (**Teorema Fundamental da Aritmética**). *Todo inteiro maior do que 1 pode ser representado de maneira única (a menos da ordem) como um produto de fatores primos.*

Dem. Se n é primo não há nada a ser demonstrado. Suponhamos então n composto. Seja p_1 ($p_1 > 1$) o menor dos divisores positivos de n. Afirmamos que p_1 é primo. Isto é verdade, pois, caso contrário p_1 seria composto, logo existiria p tal que $p|p_1$ e assim $p|n$ o que é absurdo. Portanto $n = p_1 \cdot n_1$.

Se n_1 for primo a prova está completa. Caso contrário, tomamos p_2 como o menor fator de n_1. Pelo argumento anterior, p_2 é primo e temos que $n = p_1 \cdot p_2 \cdot n_2$. Repetindo este procedimento, obtemos uma sequência decrescente de inteiros positivos $n_1, n_2, ..., n_r$. Como todos eles são inteiros maiores do que 1, este processo deve terminar. Como os primos na sequência p_1, p_2,..., p_k não são, necessariamente, distintos, n terá, em geral, a forma:

$$p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}$$

Para mostrarmos a unicidade usamos indução em n. Para $n = 2$ a afirmação é verdadeira. Assumimos, então, que ela se verifica para todos os inteiros maiores do que 1 e menores do que n. Vamos provar que ela também é verdadeira para n. Se n é primo, não há nada a provar. Vamos supor, então, que n seja composto e que tenha duas fatorações, isto é,

$$n = p_1 \cdot p_2 \cdot n_2 \cdot ... \cdot p_s = q_1 \cdot q_2 \cdot ... \cdot q_r.$$

Vamos provar que $s = r$ e que cada p_i é igual a algum q_j. Como p_i divide o produto $q_1 \cdot q_2 ... q_r$,pela Proposição 1.25, ele divide pelo menos um dos fatores q_j. Sem perda de generalidade podemos supor que $p_1 | q_1$. Como são ambos primos, isto implica $p_1 = q_1$. Logo $\frac{n}{p_1} = p_2 ... p_s = q_2 ... q_r$. Como $1 < \frac{n}{p_1} < n$, a hipótese de indução nos diz que as duas fatorações são idênticas, isto é $s = r$ e, a menos da ordem, as fatorações $p_1 \cdot p_2 \cdot ... \cdot p_s$ *e* $q_1 \cdot q_2 \cdot ... \cdot q_s$ são iguais.

■

Definição 1.27. Um número natural é um múltiplo comum de dois números inteiros dados se ele é simultaneamente múltiplo de ambos os números. Os números $a \cdot b$ e 0 são sempre múltiplos comuns de a e b.

Definição 1.28. Definiremos que um número natural m é um *mínimo múltiplo comum* (mmc) dos números inteiros a e b, ambos não nulos e denotado por $m = [a, b]$ se possuir as seguintes propriedades:

i. m é um múltiplo comum de a e b, e

ii. se c é um múltiplo comum de a e b, então $m | c$.

Exemplo 1.29. Por exemplo, 40 é um múltiplo comum de 5 e 4, mas não é um mmc destes números. O número 20 é um mmc de 5 e 4.

Se m e m' são dois mínimos múltiplos comuns de a e b, então, do item **ii.** da definição acima, temos que $m|m'$ e $m'|m$. Como m e m' são números naturais, temos que $m \leq m'$ e $m' \leq m$, logo $m = m'$, portanto se existe mínimo múltiplo comum, ele é único e é o menor dos múltiplos comuns positivos de a e b.

Teorema 1.30. *Se dois inteiros positivos a e b possuem as fatorações*

$$a = \prod_{i=1}^{n} p_i^{\alpha_i} \ e \ b = \prod_{j=1}^{n} p_j^{\beta_j}$$

então

$$(a, b) = \prod_{i=1}^{n} p_i^{\gamma_i} \ e \ [a, b] = \prod_{i=1}^{n} p_i^{\delta_i}$$

onde $\gamma_i = min\{\alpha_i, \beta_i\}$ e $\delta_i = max\{\alpha_i, \beta_i\}$.

Dem. Considere os inteiros positivos a e b tais que

$$a = \prod_{i=1}^{n} p_i^{\alpha_i} \ e \ b = \prod_{i=1}^{n} p_i^{\beta_i}$$

onde p_i é um número primo. Considere agora os inteiros d e m tais que

$$d = \prod_{i=1}^{n} p_i^{\gamma_i} \ e \ m = \prod_{i=1}^{n} p_i^{\delta_i}$$

onde $\gamma_i = min\{\alpha_i, \beta_i\}$ e $\delta_i = max\{\alpha_i, \beta_i\}$. Primeiro vamos mostrar que $d = (a, b)$. Note que $d|a$ e $d|b$ pois, como $\gamma_i = min\{\alpha_i, \beta_i\}$, então $p^{\gamma_i}|p^{\alpha_i}$ e $p^{\gamma_i}|p^{\beta_i}$, assim pela Proposição 1.5, $d|a$ e $d|b$.

Nosso próximo passo é mostrar que para todo inteiro d', talque $d'|a$ e $d'|b$ implica $d'|d$. De fato, pois se $d'|a$ e $d'|b$ então

$$d' = \prod_{i=1}^{n} p_i^{k_i}$$

onde $k_i \leq \alpha_i$, e $k_i \leq \beta_i$, logo $k_i \leq min\{\alpha_i, \beta_i\}$, para todo i e portanto $d'|d$.

Agora vamos mostrar que $m = [a, b]$. Vamos começar mostrando que m é múltiplo de a e de b. Isso é fato pois se $\delta_i = max\{\alpha_i, \beta_i\}$ então $p^{\beta_i}|p^{\delta_i}$ e $p^{\alpha_i}|p^{\delta_i}$, assim, pela Proposição 1.5, $a|m$ e $b|m$.

Para finalizar devemos mostrar que para todo inteiro m', tal que m' é múltiplo de a e de b implica $m|m'$.

Seja m' um inteiro múltiplo de a e de b, então

$$m' = \prod_{i=1}^{n} p_i^{\theta_i}$$

onde $\theta_i \geq \alpha_i,$ e $\theta_i \geq \beta_i$, logo $\theta_i \geq max\{\alpha_i, \beta_i\}$ para todo i. Portanto $m|m'$ e $m = [a, b]$.

■

Teorema 1.31. *Dados dois números inteiros a e b, ambos não nulos, temos que $[a, b]$ existe e*

$$[a, b] \cdot (a, b) = a \cdot b.$$

Dem. Vamos supor que a e b tenham fatorações dadas por

$$a = \prod_{i=1}^{n} p_i^{\alpha_i} \ e \ b = \prod_{j=1}^{n} p_j^{\beta_j}$$

.

Pelo Teorema 1.30 temos que

$$(a, b) = p_1^{min\{\alpha_1,\beta_1\}} \cdot p_2^{min\{\alpha_2,\beta_2\}} \cdot ...p_n^{min\{\alpha_n,\beta_n\}}$$

e

$$[a, b] = p_1^{max\{\alpha_1,\beta_1\}} \cdot p_2^{max\{\alpha_2,\beta_2\}} \cdot ...p_n^{max\{\alpha_n,\beta_n\}}$$

Assim

$$[a, b] \cdot (a, b) = \prod_{i=1}^{n} p_n^{min\{\alpha_n,\beta_n\}+max\{\alpha_n,\beta_n\}} = \prod_{i=1}^{n} p_i^{\alpha_i+\beta_1} = a \cdot b$$

■

2 Divisão de Polinômios de Uma Variável

Nesse capítulo vamos dar a definição de *Anéis*, *Corpos*, *Polinômios de Uma Variável*, mostraremos o algoritmo da divisão para polinômios de uma variável do mesmo modo que é feito no Ensino Médio, o algoritmo para determinar o *Máximo Divisor Comum* de polinômios e os critérios de irredutibilidade.

2.1 Anéis e Corpos

Definição 2.1. Um anel $(A, +, \cdot)$ é um conjunto A com pelo menos dois elementos, munidos de uma operação denotada por $+$ (chamada adição) e de outra operação denotada por $\cdot$ (chamada multiplicação)que satisfazem as condições seguintes:

A.1) A adição é associativa, isto é, para todo x, y, $z \in A$, $(x + y) + z = x + (y + z)$

A.2) Existe um elemento neutro com respeito à adição, isto é, existe $0 \in A$ tal que, para todo $x \in A$, $0 + x = x$ e $x + 0 = x$.

A.3) Todo elemento de A possui um inverso com respeito á adição, isto é, para todo $x \in A$, existe $z \in A$ tal que $x + z = 0$ e $z + x = 0$.

A.4) A adição é comutativa, isto é, existem x, $y \in A$ tal que $x + y = y + x$.

M.1) A multiplicação é associativa, isto é, para todo x, y, $z \in A$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

AM) A adição é distributiva relativamente à multiplicação ,isto é, para todo x, y, $z \in A$, $x \cdot (y + z) = x \cdot y + x \cdot z$.

Definição 2.2. Se A é um anel e se existir um elemento neutro com respeito à multiplicação, isto é, existe $1 \in A$ tal que, para todo $x \in A$, $1 \cdot x = x \cdot 1 = x$, dizemos que A é um anel com unidade 1.

Definição 2.3. Se A é um anel e se a multiplicação for comutativa, isto é, para todo x, $y \in A$ temos que $x \cdot y = y \cdot x$, dizemos que A é um anel comutativo.

Exemplo 2.4. $M_{n\times n}(\mathbb{R}) = (a_{ij})$, onde $i,\ j = 1, ..., n$ é anel e $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, são anéis comutativos.

Definição 2.5. Um anel $(K, +, \cdot)$ é chamado *Corpo* se ele satisfaz a seguinte condição: Todo elemento diferente de zero de K possui um inverso com respeito à multiplicação, isto é, todo $x \in K \setminus \{0\}$,existe $y \in K$ tal que $x \cdot y = 1$.

Exemplo 2.6. $(\mathbb{Q}, +, \cdot)$ e $(\mathbb{R}, +, \cdot)$ são *Corpos*.

2.2 Polinômios de Uma Variável e O algoritmo da Divisão

Nesta seção, vamos discutir *polinômios de uma "variável"* (ou *"indeterminada"*) e apresentar *O algoritmo a divisão álgebrica* de polinômios em uma varável.

Definição 2.7. Seja K um corpo qualquer. Chamamos de um *polinômio* sobre K em uma variável x a uma expressão formal $p(x) = a_0 + a_1x + ... + a_mx^m + ...$ onde $a_i \in K$, para todo $i \in \mathbb{N}_0$ e existe $n \in \mathbb{N}$ tal que $a_j = 0$ para todo $j > n$. Neste caso, denotaremos $p(x) = a_0 + a_1x + ... + a_nx^n$ onde $a_n \neq 0$.

Por exemplo: $p\,(x) = 2x^5 - 19x^4 - \frac{7}{9}x^3 - \sqrt[3]{14}x^2 + x + 2$ é um polinômio sobre $\mathbb{R}$ e $q\,(x) = 2ix^2 - (9 + i)\,x + 3$ é um polinômio sobre $\mathbb{C}$.

Dizemos que dois polinômios $p(x) = a_0 + a_1x + ... + a_mx^m$ e $q(x) = b_0 + b_1x + ... + b_kx^k$ sobre K são iguais se e somente se $a_i = b_i$ em K, para todo $i \in \mathbb{N}_0$.

Se $p\,(x) = 0 + 0x + ... + 0x^m$ indicaremos $p(x)$ por 0 e o chamamos de *o polinômio identicamente nulo* sobre K. Assim um polinômio $p(x) = a_0 + a_1x + ... + a_mx^m$ sobre K é identicamente nulo se e somente se $a_i = 0 \in K$para todo $i \in \mathbb{N}_0$.

Se $a \in K$ indicaremos por a ao polinômio $p(x) = a_0 + a_1x + ... + a_mx^m$ onde $a_0 = a$, e $a_i = 0$ para todo $i \geq 1$. Chamamos ao polinômio $p(x) = a$, $a \in K$ de *polinômio constante* a.

Exemplo 2.8. Por exemplo o polinômio $p\,(x) = -\frac{5}{3}$ é chamado de polinômio contante $-\frac{5}{3}$.

Definição 2.9. Seja $p\,(x) = a_0 + a_1x + ... + a_nx^n$ um polinômio tal que $a_n \neq 0$

i. chamamos a_i de *coeficiente* do monômio x^i.

ii. se $a_i \neq 0$, chamamos a_ix^i de *termo* de $p\,(x)$.

iii. n é o *grau do polinômio* $p\,(x)$, e nesse caso indicamos o grau de $p\,(x)$ por $\partial\,(p) = n$.

Exemplo 2.10. Considere $p(x) = -9x^3 - 4x^2 + 3x - 1$ um polinômio sobre $\mathbb{R}$, então:

i. $-9,\ -4,\ 3$ e -1 são os coeficientes de $p(x)$;

ii. $-9x^3,\ -4x^2,\ 3x$ e -1 são termos de $p(x)$;

iii. 3 é o *grau do polinômio* $p(x)$, ou seja $\partial(p) = 3$.

Vamos denotar por $K[x]$ o conjunto de todos os polinômios sobre K em uma variável x. Observe que não está definido o grau do polinômio 0, e ∂ pode ser interpretada como uma função do conjunto de todos os polinômios não nulos sobre o conjunto $\mathbb{N}_0$. Assim,

$$\partial : K[x] - \{0\} \longrightarrow \mathbb{N}_0$$

$$p(x) \longmapsto \partial(p) = grau\ de\ p(x)$$

Agora vamos definir operações soma e produto no conjunto $K[x]$.

Definição 2.11. Sejam $p(x) = a_0 + a_1x + ... + a_mx^m$ e $q(x) = b_0 + b_1x + ... + b_kx^k$ dois elementos do conjunto $K[x]$. Definimos

$$p(x) + q(x) = c_1 + ... + c_kx^k\ onde\ c_i = (a_i + b_i) \in K$$

e

$$p(x) \cdot q(x) = c_0 + ... + c_kx^k$$

onde

$$c_0 = a_0b_0,\ c_1 = a_0b_1 + a_1b_0,\ c_2 = a_0b_2 + a_1b_1 + a_2b_0, ...,$$
$$c_k = a_0b_k + a_1b_{k-1} + ... + a_{k-1}b_1 + a_kb_0,\ k \in \mathbb{N}_0$$

A definição de produto provém da regra $x^m \cdot x^n = x^{m+n}$ e da propriedade distributiva. Convencionam-se também as regras $x^0 = 1$ e $x^1 = x$.

Note que $(K[x], +, \cdot)$ é um anel comutativo.

Exemplo 2.12. Considere $a(x) = x^3 + \frac{4}{17}x^2 - x + 13$ e $b(x) = x^2 + 4x$ polinômios sobre $\mathbb{R}$, então

$$\begin{aligned} s(x) = &\ a(x) + b(x) = \\ = &\ x^3 + \left(\tfrac{4}{17} + 1\right)x^2 + (-1 + 4)x + 13 = \\ = &\ x^3 + \tfrac{21}{17}x^2 + 3x + 13 \end{aligned}$$

e

$$\begin{aligned} p(x) = &\ a(x) \cdot b(x) = \\ = &\ x^3 \cdot (x^2 + 4x) + \tfrac{4}{17}x^2 \cdot (x^2 + 4x) - x \cdot (x^2 + 4x) + 13 \cdot (x^2 + 4x) = \\ = &\ x^5 + 4x^4 + \tfrac{4}{17}x^4 + \tfrac{16}{17}x^3 - x^3 - 4x^2 + 13x^2 + 52 = \\ = &\ x^5 + \tfrac{72}{17}x^4 - \tfrac{1}{17}x^3 + 9x^2 + 52 \end{aligned}$$

Proposição 2.13. *Sejam $f(x)$ e $g(x)$ polinômios em $K[x]$. A função grau ∂, possui as seguintes propriedades:*

i. *$\partial(f+g) \leq max\{\partial(f), \partial(g)\}$, quaisquer que sejam os polinômios não nulos $f(x)$ e $g(x) \in K[x]$ tais que $f(x) + g(x) \neq 0$.*

ii. *$\partial(f \cdot g) = \partial(f) + \partial(g)$, quaisquer que sejam os polinômios não nulos $f(x)$ e $g(x) \in K[x]$.*

Dem. Sejam $f(x)$ e $g(x)$ polinômios em $K[x]$, tais que

$$f(x) = \sum_{i=0}^{n} a_i x^i \text{ e } g(x) \sum_{j=0}^{m} b_j x^j.$$

Vamos supor sem perda de generalidade que $n \geq m$.

(i.) Temos que

$$f(x) + g(x) = \sum_{i=0}^{n} a_i x^i + \sum_{j=0}^{m} b_j x^j = a_0 + a_1 x + ... + a_n x^n + b_0 + b_1 x + ... + b_m x^m.$$

Se $n = m$ então

$$\begin{aligned} f(x) + g(x) = &\ a_0 + a_1 x + ... + a_n x^n + b_0 + b_1 x + ... + b_n x^n = \\ = &\ (a_0 + b_0) + (a_1 + b_1) x + ... + (a_n + b_n) x^n = \\ = &\ c_0 + c_1 x + ... + c_n x^n \end{aligned}$$

onde $c_i = a_i + b_i$, portanto $\partial(f+g) \leq n = max\{\partial(f), \partial(g)\}$.

Se $n > m$ então

$$\begin{aligned} f(x) + g(x) = &\ a_0 + a_1 x + ... + a_m x^m + ... + a_n x^n + b_0 + b_1 x + ... + b_n x^n = \\ = &\ (a_0 + b_0) + (a_1 + b_1) x + ... + (a_m + b_m) x^m + ... + a_n x^n = \\ = &\ c_0 + c_1 x + ... + c_m x^m + ... + a_n x^n \end{aligned}$$

onde $c_i = a_i + b_i$, para $i = 1,\ 2,\ ...,\ n$, portanto $\partial(f+g) = n = max\{\partial(f), \partial(g)\}$.

(ii.) Considere agora

$$f(x) \cdot g(x) = \sum_{i=0}^{n} a_i x^i \cdot \sum_{j=0}^{m} b_j x^j = (a_0 + a_1 x + ... + a_n x^n) \cdot (b_0 + b_1 x + ... + b_m x^m)$$

aplicando a propriedade distributiva do item **AM** da definição 2.1 temos que

$$\begin{aligned} f(x) \cdot g(x) = &\quad a_0 \cdot (b_0 + b_1 x + ... + b_m x^m) + \\ +a_1 x \cdot (b_0 + b_1 x + ... + b_m x^m) + &\quad ... + a_n x^n \cdot (b_0 + b_1 x + ... + b_m x^m) = \\ = a_0 b_0 + (a_0 b_1 + a_1 b_0) x + &\quad (a_0 b_2 + a_1 b_1 + a_2 b_0) x^2 + ... + a_n b_m x^{n+m}, \end{aligned}$$

e portanto, $\partial(f \cdot g) = n + m = \partial(f) + \partial(g)$.

■

Observação 2.14. Da proposição acima segue que os únicos polinômios invertíveis em $K[x]$ são os polinômios constantes não nulos.

Exemplo 2.15. Como vimos no Exemplo 2.12,

$$3 = \partial(s) = \partial(a+b) \leq max\{\partial(a), \partial(b)\} = 3$$

e

$$5 = \partial(p) = \partial(a \cdot b) = \partial(f) + \partial(g) = 3 + 2 = 5$$

Definição 2.16. Seja $p(x) = a_0 + a_1 x + ... + a_m x^m \in K[x]$ um polinômio de grau m. Então dizemos que $a_m x^m$ é o *termo líder* de $p(x)$, e escrevemos $TL(p) = a_m x^m$.

Teorema 2.17. *(O algoritmo da divisão). Seja K um corpo e seja $d(x)$ um polinômio em $K[x]$. Então todo $p(x) \in K[x]$ pode ser escrito como*

$$p(x) = d(x) \cdot q(x) + r(x),$$

em que $q(x)$ e $r(x) \in K[x]$ e $r(x) = 0$ ou $\partial(r) < \partial(d)$. Além disso, $q(x)$ e $r(x)$ são únicos e há um algoritmo para encontrar $q(x)$ e $r(x)$.

Dem. Sejam os polinômios $d(x)$ e $p(x) \in K[x]$. Considere agora que

$$q_1(x) = 0 \text{ e } r_1(x) = p(x)$$

se $\partial(p) < \partial(d)$ o algoritmo termina e $q(x) = q_1(x)$ e $r(x) = r_1(x)$.

Caso contrário temos que

$$p(x) = q_1(x) \cdot d(x) + r_1(x),$$

e daí, tomamos

$$q_2(x) = q_1(x) + TL(r_1)/TL(d)$$

e

$$r_2(x) = r_1(x) - (TL(r_1)/TL(d)) \cdot d(x).$$

Se $r_2 = 0$ ou se $\partial(r_2) < \partial(d)$ o algoritmo termina e $q(x) = q_2(x)$ e $r(x) = r_2(x)$.

Caso contrário temos que

$$p(x) = q_2(x) \cdot d(x) + r_2(x),$$

e daí, tomamos

$$q_3(x) = q_2(x) + TL(r_2)/TL(d)$$

e

$$r_3(x) = r_2(x) - (TL(r_2)/TL(d)) \cdot d(x).$$

Se $r_3 = 0$ ou se $\partial(r_3) < \partial(d)$ o algoritmo termina e $q(x) = q_3(x)$ e $r(x) = r_3(x)$.

Esse processo deve ser repetido enquanto $r_i(x) \neq 0$ e $TL(d)$ dividir $TL(r_i)$, ou seja, o algoritmo termina somente quando $r_i(x)$ apresentar as propriedades requeridas, daí então:

$$q(x) = q_i(x) \text{ e } r(x) = r_i(x)$$

O algoritmo funciona pois é verdadeiro para os valores iniciais $q_1(x)$ e $r_1(x)$ e além disso toda vez que redefinimos os valores de $q_i(x)$ e $r_i(x)$, a igualdade

$$p(x) = d(x) \cdot q_i(x) + r_i(x)$$

continua verdadeira devido à identidade

$$p(x) = d(x) \cdot q(x) + r(x) = [q(x) + TL(r)/TL(d)] \cdot d(x) + [r(x) - (TL(r)/TL(d)) \cdot d(x)]$$

Para mostrar que o algoritmo realmente termina, basta notar que

$$r(x) - (TL(r)/TL(d)) \cdot d(x)$$

é 0 ou tem grau menor que $r(x)$. Para mostrar isso, suponha que

$$r(x) = a_0 + a_1x + ... + a_mx^m$$

e

$$d(x) = b_0 + b_1x + ... + b_kx^k$$

e suponha que $m \geq k$, então

$$r'(x) = r(x) - (TL(r)/TL(d)) \cdot d(x) =$$

$$(a_0 + a_1x + ... + a_mx^m) - (a_m/b_k) \cdot x^{m-k} \cdot \left(b_0 + b_1x + ... + b_kx^k\right) \tag{2.1}$$

segue da equação (2.1) que o grau de $r'(x)$ diminui (ou toda expressão desaparece). Continuando esse processo, pelo *Princípio da Boa Ordem*, em algum momento temos que $\partial(r_i) < \partial(d)$ ou $r_i = 0$, o que prova que o algoritmo termina.

Para finalizar a demonstração vamos mostra que $q(x)$ e $r(x)$ são únicos.

Suponha que $p(x) = d(x) \cdot q(x) + r(x) = d(x) \cdot q'(x) + r'(x)$ onde $r(x)$ e $r'(x)$ tenham graus menores que o grau de $d(x)$ (ou um deles é 0, ou ambos são 0).

Se $r(x) \neq r'(x)$, então $\partial(r - r') < \partial(d)$. Por outro lado

$$(q(x) - q'(x)) \cdot d(x) = r'(x) - r(x) \tag{2.2}$$

e teríamos $q(x) - q'(x) \neq 0$, consequentemente

$$\partial(r' - r) = \partial(q - q') \cdot d(x) = \partial(q - q') + \partial(d) \geq \partial(d)$$

o que é absurdo, logo $r(x) = r'(x)$ e, por (2.2), $q'(x) = q(x)$. Assim a demonstração está completa.

■

Exemplo 2.18. Considere $p(x)$ e $d(x) \in \mathbb{R}[x]$, onde $p(x) = 7x^4 - 5x^3 + 12x^2 + 6x - 8$ e $d(x) = x^2 - 3x + 1$. Vamos encontrar $q(x)$, $r(x) \in \mathbb{R}[x]$ tais que

$$p(x) = q(x) \cdot d(x) + r(x)$$

Vamos usar o resultado do Teorema 2.17, sendo assim temos

$$q_1(x) = 0 \ e \ r_1(x) = 7x^4 - 5x^3 + 12x^2 + 6x - 8$$

como $r_1(x) \neq 0$ e $\partial(r_1) = 4 \geq 2 = \partial(d)$ devemos continuar, então

$$q_2(x) = q_1(x) + TL(r_1)/TL(d) = 0 + 7x^4/x^2 = 7x^2$$

e

$$\begin{gathered} r_2(x) = r_1(x) - (TL(r_1)/TL(d)) \cdot d(x) = \\ = 7x^4 - 5x^3 + 12x^2 + 6x - 8 - (7x^4/x^2) \cdot (x^2 - 3x + 1) = \\ = 16x^3 + 5x^2 + 6x - 8 \end{gathered}$$

como $r_2(x) \neq 0$ e $\partial(r_2) = 3 \geq 2 = \partial(d)$ devemos continuar, então

$$q_3(x) = q_2(x) + TL(r_1)/TL(d) = 7x^2 + 16x^3/x^2 = 7x^2 + 16x$$

e

$$\begin{aligned} & r_3(x) = r_2(x) - (TL(r_2)/TL(d)) \cdot d(x) = \\ & = 16x^3 + 5x^2 + 6x - 8 - (16x^3/x^2) \cdot (x^2 - 3x + 1) = \\ & = 53x^2 - 10x - 8 \end{aligned}$$

como $r_3(x) \neq 0$ e $\partial(r_3) = 2 = \partial(d)$ devemos continuar, então

$$q_4(x) = q_3(x) + TL(r_3)/TL(d) = 7x^2 + 16x + 53x^2/x^2 = 7x^2 + 16x + 53$$

e

$$\begin{aligned} & r_4(x) = r_3(x) - (TL(r_3))/TL(d)) \cdot d(x) = \\ & = 53x^2 - 10x - 8 - (53x^2/x^2) \cdot (x^2 - 3x + 1) = 149x - 61 \end{aligned}$$

como $\partial(r_4) = 1 < 2 = \partial(d)$ chegamos ao resultado desejado, ou seja

$$q(x) = 7x^2 + 16x + 53 \text{ } e \text{ } r(x) = 149x - 61$$

logo

$$7x^4 - 5x^3 + 12x^2 + 6x - 8 = \left(7x^2 + 16x + 53\right) \cdot \left(x^2 - 3x + 1\right) + 149x - 61$$

Corolário 2.19. *Se K é um corpo e $p(x) \in K[x]$ é um polinômio diferente de zero, então $p(x)$ tem no máximo $\partial(p)$ raízes em K.*

Dem. Vamos usar a indução de $m = \partial(p)$. Quando $m = 0$, $p(x)$ é uma constante diferente de zero, então o corolário é obviamente verdadeiro. Agora, vamos supor que o

corolário vale para todos os polinômios de grau $m-1$, e seja $p(x)$ com grau m. Se $p(x)$ não tem raízes em K, então não há nada a ser demonstrado. Então, suponhamos que a é uma raiz em K. Se dividirmos $p(x)$ por $x-a$, então, o algoritmo da divisão nos diz que $p(x) = q(x) \cdot (x-a) + r(x)$, onde $r(x) \in K$ já que $x-a$ tem grau 1. Para determinar $r(x)$, vamos substituir em ambos os lados $x = a$, o que dá $0 = p(a) = q(a) \cdot (a-a) + r = r$. Daí resulta que $p(x) = q(x) \cdot (x-a)$. Note também que $q(x)$ tem grau $m-1$.

Afirmamos que qualquer raíz de $p(x)$ que não seja a também é uma raíz de $q(x)$. Para ver isto, tome $b \neq a$ uma raíz de $p(x)$. Então, $0 = p(b) = q(b) \cdot (b-a)$ o que implica que $q(b) = 0$ uma vez que K é um corpo. Como $q(x)$ tem no máximo $m-1$ raízes por nossa suposição indutiva, $p(x)$ tem no máximo m raízes em K. Isso completa a prova.

■

Definição 2.20. O *Máximo Divisor Comum* (MDC) dos polinômios $a(x), b(x) \in K[x]$ é um polinômio $d(x)$ tal que:

i. $d(x)$ divide $a(x)$ e $b(x)$.

ii. Se $d'(x)$ é um outro polinômio que divide $a(x)$ e $b(x)$, então $d'(x)$ divide $d(x)$.

Quando $d(x)$ tem essas propriedades, podemos escrever $d(x) = (a, b)$.

Proposição 2.21. *Seja K um corpo. Sejam $a(x), b(x) \in K[x]$. Então $a(x) \,|\, b(x)$ se, e somente se, $(a, b) = a(x)$.*

Dem. Se $a(x) \,|\, b(x)$, então $a(x)$ é um divisor comum de $a(x)$ e $b(x)$, e, se $c(x)$ é um divisor comum de $a(x)$ e $b(x)$, então $c(x)$ divide $a(x)$, o que mostra que $a(x) = (a, b)$. Por outro lado, se $(a, b) = a(x)$, segue-se que $a(x)$ divide $b(x)$, logo $a(x) \,|\, b(x)$.

■

Proposição 2.22. *Seja K um corpo. Considere os polinômios $a(x), b(x), n(x) \in K[x]$. Se existe $(a, b - n \cdot a)$, então (a, b) existe e $(a, b) = (a, b - n \cdot a)$:*

Dem. Seja $d(x) = (a, b - n \cdot a)$. Como $d(x) \,|\, a(x)$ e $d(x) \,|\, (b(x) - n(x) \cdot a(x))$, segue que $d(x)$ divide $b(x) = b(x) - n(x) \cdot a(x) + n(x) \cdot a(x)$. Logo, $d(x)$ é um divisor comum de $a(x)$ e $b(x)$. Suponha agora que $c(x)$ seja um divisor comum de $a(x)$ e $b(x)$. Logo, $c(x)$ é um divisor comum de $a(x)$ e $b(x) - n(x) \cdot a(x)$ e, portanto, $c(x) \,|\, d(x)$, assim demonstramos que $d(x) = (a, b)$.

■

Proposição 2.23. *Seja K um corpo e sejam os polinômios $a(x)$, $b(x) \in K[x]$. Então (a, b) existe e é único a menos de uma multiplicação por uma constante $k \in K$.*

Dem. Seja K um corpo e sejam os polinômios $a(x)$, $b(x) \in K[x]$ tais que $\partial(a) \leq \partial(b)$. Se $a(x) | b(x)$, temos que $(a, b) = a(x)$. Se $a(x) \nmid b(x)$ então, pelo algoritmo da divisão, podemos escrever

$$b(x) = a(x) \cdot q_1(x) + r_1(x), \ com\ 0 \leq \partial(r_1) < \partial(a).$$

Temos duas possibilidades:

1. Se $r_1(x) | a(x)$, pela Proposição 2.21 e pela Proposição 2.22,

$$r_1(x) = (a, r_1) = (a, b - q_1 \cdot a) = (a, b)$$

   e termina o algoritmo.

2. Se $r_1(x) \nmid a(x)$, podemos efetuar a divisão de $a(x)$ por $r_1(x)$, obtendo

$$a(x) = r_1(x) \cdot q_2(x) + r_2(x), \ com\ 0 \leq \partial(r_2) < \partial(r_1)$$

Novamente, temos duas possibilidades:

1. Se $r_2(x) | r_1(x)$, pela Proposição 2.21 e pela Proposição 2.22,

$$r_2(x) = (r_2, r_1) = (r_1, a - q_2 \cdot r_1) = (r_1, a) = (a, b - q_1 \cdot a) = (a, b)$$

   e termina o algoritmo.

2. Se $r_2(x) \nmid r_1(x)$, podemos efetuar a divisão de $r_1(x)$ por $r_2(x)$, obtendo

$$r_1(x) = r_2(x) \cdot q_3(x) + r_3(x), \ com\ 0 \leq \partial(r_3) < \partial(r_2)$$

Este procedimento não pode continuar indefinidamente, pois teríamos uma sequência de números naturais $\partial(a) > \partial(r_1) > \partial r_2(x) > ...$ que não possui menor elemento, o que não é possível pela *Propriedade da Boa Ordem*. Logo, para algum n, temos que $r_n(x) | r_{n-1}(x)$, logo $(a, b) = (a, r_1) = (r_1, r_2) = (r_2, r_3) = (r_{n-1}, r_n) = r_n(x)$. Dessa forma demonstramos de forma construtiva a existência do *MDC* dos polinômios $a(x)$ e $b(x)$ em $k[x]$.

Vamos demonstrar agora a unicidade. Considere $m(x)$, $m'(x) \in K[x]$ tais que $m(x) = (a, b)$ e $m'(x) = (a, b)$. Por definição $m(x) | m'(x)$ e $m'(x) | m(x)$, logo $\partial(m) = \partial(m')$. Então $m(x) = k_1 \cdot m'(x)$ e $m'(x) = k_2 \cdot m(x)$ $, k_1,\ k_2 \in K$.

■

Observação 2.24. A demonstração da Proposição 2.23 é um algoritmo que permite encontra o *MDC* entre dois polinômios de uma variável.

Exemplo 2.25. Vamos encontrar $m(x)$ o *MDC* de $a(x) = x^2 + 6x + 2x + 8$ e $b(x) = 5x^3 + 24x^2 + 25x - 6$ polinômios em $\mathbb{Q}[x]$.

Pelo 2.17 existem $q_1(x)$ e $r_1(x)$ tais que

$$b(x) = q_1(x) \cdot a(x) + r_1(x)$$

efetuando a divisão de $b(x)$ por $a(x)$temos

$5x^3 + 24x^2 + 25x - 6$	$x^2 + 6x + 8$
$-5x^3 - 30x^2 - 40x$	$q_1 = 5x - 6$
$0 - 6x^2 - 15x - 6$	
$6x^2 + 36x + 48$	
$r_1 = 21x + 24$	

como $r_1(x) \neq 0$ devemos efetuar a divisão de $a(x)$ por $r_1(x)$, ou seja:

$x^2 + 6x + 8$	$21x + 42$	$\longleftarrow$ MDC
$-x^2 - 2x$	$q_2 = \frac{x}{21} + \frac{4}{21}$	
$0 + 4x + 8$		
$-4x - 8$		
$r_2 = 0$		

como $r_2 = 0$ o algoritmo termina e $m(x) = 21x + 42$.

Definição 2.26. Seja $p(x) \in K[x]$ tal que $\partial(p) \geq 1$. Dizemos que $p(x)$ é um *polinômio irredutível* sobre K se toda vez que $p(x) = g(x) \cdot h(x)$, $g(x)$, $h(x) \in K[x]$ então temos $g(x) = a$ constante em K ou $h(x) = b$ constante em K. Se $p(x)$ for *não irredutível* sobre K dizemos que $p(x)$ é *redutível* sobre K.

Obviamente todo polinômio de grau 1 sobre um corpo K é irredutível sobre K. Observe também que o polinômio $p(x) = x^2 + 1$ é irredutível sobre o corpo $\mathbb{Q}$ porém é redutível sobre $\mathbb{C}$.

2.3 Fatoração Única

Seja $u \in K - \{0\}$ e sejam $p_1(x), ..., p_m(x)$ polinômios irredutíveis sobre K vamos usar a expressão $p(x) = u \cdot p_1(x) \cdot ... \cdot p_m(x)$, incluindo na mesma a possibilidade, no caso de $m = 0$, $p(x) = u$.

Proposição 2.27. *Sejam f(x), $g(x) \in K[x]$, então existem a(x), $b(x) \in K[x]$ tais que* $(f, g) = a(x) \cdot f(x) + b(x) \cdot g(x)$.

Dem. Seja $d(x) = a_1(x) \cdot f(x) + b_1(x) \cdot g(x), \in K[x]$ tal que $\partial(d) \leq \partial(d')$, para todo $d'(x) \in K[x]$.

Se $d(x) | f(x)$ e se $d(x) | g(x)$ então $d(x) = (f, g)$. Suponha então que $d(x) \nmid f(x)$, logo existem *q(x)*, $r(x) \in K[x]$ tais que $f(x) = q(x) d(x) + r(x)$, onde $\partial(r) < \partial(d)$. Assim

$$\begin{aligned} & r(x) = f(x) - d(x) \cdot q(x) = \\ & = f(x) - q(x) \cdot [a_1(x) \cdot f(x) + b_1(x) \cdot g(x)] = \\ & = f(x) \cdot [1 - q(x) \cdot a_1(x)] + b_1(x) \cdot g(x) \end{aligned}$$

com $\partial(r) < \partial(d)$ o que é absurdo, logo $d(x) | f(x)$, $d(x) | g(x)$.

Seja $d'(x) \in K[x]$ divisor comum de *f(x)*, *g(x)*, então $f(x) = d'(x) \cdot a(x)$, $g(x) = d'(x) \cdot b(x)$ o que implica que

$$d(x) = a_1(x) \cdot f(x) + b_1(x) \cdot g(x) = [a_1(x) \cdot a(x)] \cdot d'(x) + [b_1(x) \cdot b(x)] \cdot d'(x)$$

o que implica que $d(x)$ é (f, g)

■

Proposição 2.28. *Seja $f(x) \in K[x]$ um polinômio irredutível e suponha que $f(x)$ divide o produto $g(x) \cdot h(x)$, onde g(x), $h(x) \in K[x]$. Então $f(x)$ divide $g(x)$ ou $h(x)$.*

Dem. Se $f(x)$ divide $g(x) \cdot h(x)$, então considere $p(x) = MDC(f, g)$. Se $g(x) \cdot h(x)$ é um polinômio não constante, então $f(x)$ deve ser um múltiplo constante de $p(x)$ uma vez que $f(x)$ é irredutível, e segue-se que $f(x)$ divide $g(x)$. Por outro lado, se $p(x)$ é uma constante, podemos assumir $p(x) = 1$, e então pela Proposição 2.27 nós podemos encontrar *a*, $\in K[x]$ tal que $a(x) f(x) + b(x) g(x) = 1$. Se multiplicarmos por *h(x)*, obtemos

$$h(x) = h(x) \cdot [a(x) \cdot f(x) + b(x) \cdot g(x)] = a(x) \cdot h(x) \cdot f(x) + b(x) \cdot g(x) \cdot h(x).$$

Como $f(x)$ divide $g(x)h(x)$, $f(x)$ é um fator de $a(x)h(x)f(x) + b(x)g(x)h(x)$, e, assim, $f(x)$ divide $h(x)$.

■

Teorema 2.29. *Seja K um corpo. Então todo polinômio $p(x) \in K[x] - \{0\}$ pode ser escrito na forma,*

$$p(x) = u \cdot p_1(x) \cdot ... \cdot p_m(x)$$

onde $u \in K - \{0\}$ e $p_1(x), p_2(x), ..., p_m(x)$ são polinômios irredutíveis sobre K. (não necessariamente distintos). Mais ainda, essa expressão é única a menos da constante u e da ordem dos polinômios $p_1(x), ..., p_m(x)$.

Dem. Seja $p(x) \in K[x] - \{0\}$. Vamos provar por indução sobre $\partial(p) = n$.

Se $n = 0$, então $p(x) = u$ constante não nula. Assim, podemos assumir $\partial(p) = n \geq 1$.

Vamos supor pela hipótese de indução que todo polinômio não nulo de grau menor que n pode ser escrito na expressão desejada, e vamos demonstrar que $p(x)$ também pode ser escrito naquela expressão.

Seja $p(x)$ um polinômio redutível sobre K, tal que $\partial(p) = n$, então existem $g(x), h(x) \in K[x]$, $1 \leq \partial(g) < n$, $1 \leq \partial(h) < n$, tais que $p(x) = g(x) \cdot h(x)$. Agora, por hipótese de indução temos,

$$g(x) = a \cdot p_1(x) \cdot ... \cdot p_r(x), \text{ e } h(x) = b \cdot p_{r+1}(x) \cdot ... \cdot p_m(x),$$

com $a, b \in K - \{0\}$ e p_i polinômios irredutíveis sobre K.

Assim, $p(x) = u \cdot p_1(x) \cdot ... \cdot p_m(x)$, onde $u = a \cdot b \in K - \{0\}$ e $p_1(x) \cdot ... \cdot p_m(x)$ polinômios irredutíveis sobre K.

Vamos agora demonstrar a unicidade da expressão.

Suponhamos

$$p(x) = u \cdot p_1(x) \cdot ... \cdot p_m(x) = u' \cdot p'_1(x) \cdot ... \cdot p'_s(x)$$

onde $u, u' \in K - \{0\}$ e $p_1(x)$, ..., $p_m(x)$, $p'_1(x)$, ..., $p'_s(x)$ são polinômios irredutíveis sobre K.

Se $m = 1$, então $s = m$ já que por hipótese p_1 é irredutível.

Vamos admitir ser verdade para $m-1$, então

$$u \cdot p_1(x) \cdot ... \cdot p_m(x) = u' \cdot p'_1(x) \cdot ... \cdot p'_s(x) \tag{2.3}$$

implica que cada p_i divide algum p_j. Sem perda de generalidade vamos supor que $p_1 | p'_1$, o que implica que existe $u_1 \in K$ tal que $p'_1 = u_1 \cdot p_1$. Simplificando $u_1 \cdot p_1$ em ambos os membros da equação 2.3, temos que

$$u_2 \cdot p_2 \cdot ... \cdot p_m = u'_2 \cdot p'_2 \cdot ... \cdot p's$$

u_2, $u'_2 \in K$.

Portanto, pela nossa hipótese de indução, $m = s$ e a expressão em fatores é única a menos da ordem dos polinômios $p_1(x)$, ..., $p_m(x)$ e da multiplicação por uma constante.

■

Em geral verificar se um polinômio é irredutível sobre um corpo é um problema difícil.

3 Divisão de Polinômios de Duas Variável

Neste capítulo vamos tratar de polinômios em várias variáveis. Vamos estabelecer ordem de monômios e algoritmo da divisão em polinômios em $K[x, y]$, e também mostrar alguns exemplos.

3.1 Ordenações em $K[x_1, \ ..., \ x_n]$

Definição 3.1. Um polinômio p em $x_1, \ ..., \ x_n$ com coeficientes em K é uma combinação linear finita (com coeficientes em K) de monômios. Vamos escrever o polinômio p na forma

$$p = \sum_{\alpha} a_\alpha x^\alpha, \ a_\alpha \in K$$

onde a soma é sobre um número finito de n-uplas $\alpha = (\alpha_1, \ ..., \ \alpha_n)$. A n-upla α será denotada por *grau total* do monômio x^i, o conjunto de todos polinômios em $x_1, \ ..., \ x_n$ com coeficientes em K será denotado por $K[x_1, \ ..., \ x_n]$.

Quando se tratar de polinômios com número pequeno de variáveis, normalmente dispensamos os subscritos. Assim, polinômios em uma, duas e três variáveis estão em $K[x]$, $K[x, \ y]$ e $K[x, \ y, \ z]$, respectivamente. Por exemplo,

$$f = 9x^4y^5z^2 + 2y^3z^4 - 5xy + 2z$$

é um polinômio em $\mathbb{Q}[x, y, z]$.

Se examinarmos em detalhes o algoritmo da divisão em $K[x]$, vemos que uma noção de ordenação dos termos dos polinômios é fundamental. Como vimos no Exemplo 2.18 dividindo $p(x) = 7x^4 - 5x^3 + 12x^2 + 6x - 8$ por $d(x) = x^2 - 3x + 1$, usando o algoritmo da divisão, fizemos o seguinte:

i. escrevemos os termos do polinômio em ordem decrescente de grau de x;

ii. no primeiro passo, o termo líder, que é o termo de maior grau em $p(x)$ é:

$$TL(p) = 7x^4 = 7 \cdot x^2 \cdot x^2 = 7 \cdot x^2 \cdot TL(d)$$

Então, subtraímos $7 \cdot x^2 \cdot d(x)$ de $p(x)$ para cancelar o termo líder, obtendo $16x^3 + 5x^2 + 6x - 8$;

iii. então, repetimos o mesmo processo sobre $p(x) - 7 \cdot x^2 \cdot d(x)$, etc. até obtermos o polinômio $r(x) = 149x - 61$ de grau menor que 2.

Logo, para o algoritmo da divisão sobre polinômios de uma variável, lidamos com a ordem de grau sobre monômios de uma variável:

$$... > x^{m+1} > x^m > ... > x^2 > x > 1.$$

Da evidência acima, podemos imaginar que uma componente muito importante de alguma extensão da divisão para polinômios arbitrários em mais de uma variavel seja uma ordem de termos em polinômios em $K[x_1, ..., x_n]$. Aqui, discutiremos as propriedades desejáveis que as ordens poderiam ter, e construiremos alguns exemplos diferentes que satisfarão essas necessidades. Cada uma destas ordens será usada em diferentes contextos.

Definição 3.2. Uma ordem monomial em $K[x_1, ..., x_n]$ é qualquer relação $>$ sobre $\mathbb{N}_0^n$ (equivalentemente, uma relação no conjunto dos monômios x^α, $\alpha \in \mathbb{N}_0^n$), satisfazendo:

i. A relação $>$ é uma ordem total (ou linear) sobre sobre $\mathbb{N}_0^n$, isto é, para todo par α, $\beta \in \mathbb{N}_0^n$, exatamente uma das três condições é verdadeira:

$$\alpha > \beta \text{ ou } \alpha = \beta \text{ ou } \alpha < \beta;$$

ii. Se $\alpha > \beta$ e $\gamma \in \mathbb{N}_0^n$, então

$$\alpha + \gamma > \beta + \gamma$$

iii $>$ é uma boa ordenação sobre $\mathbb{N}_0^n$. Isto significa que todo subconjunto não vazio de $\mathbb{N}_0^n$ tem um elemento mínimo em relação a $>$.

Dada uma tal relação $>$ sobre $\mathbb{N}_0^n$, escrevemos $x^\alpha > x^\beta$ se, e somente se, $\alpha > \beta$.

O Lema a seguir nos ajudará a entender o que a condição da boa ordenação significa.

Lema 3.3. *Uma relação de ordem $>$ sobre $\mathbb{N}_0^n$ é uma boa ordenação se, e somente se, toda sequência estritamente decrescente em $\mathbb{N}_0^n$*

$$\alpha_1 > \alpha_2 > \alpha_3 > ...$$

é finita.

Dem. Provaremos a contra-positiva: A relação $>$ não é uma boa ordenação se, e somente se, existe uma sequência infinita estritamente decrescente em $\mathbb{N}_0^n$.

($\Rightarrow$) Se $>$ não é uma boa ordenação, então algum subconjunto não vazio $S \subset \mathbb{N}_0^n$ não possui elemento mínimo. Seja $\alpha_1 \in S$. Já que α_1 não é o elemento mínimo, podemos encontrar $\alpha_2 \in S$ tal que $\alpha_1 > \alpha_2$ em S. Então α_2 também não é o elemento mínimo, logo existe $\alpha_3 \in S$ tal que $\alpha_1 > \alpha_2 > \alpha_3$ em S . Continuando este processo, conseguimos uma sequência infinita estritamente decrescente: $\alpha_1 > \alpha_2 > \alpha_3 > ....$

($\Leftarrow$) Dada uma sequência infinita estritamente decrescente, $\alpha_1 > \alpha_2 > \alpha_3 > ...$, temos que o conjunto $\{\alpha_1,\ \alpha_2,\ \alpha_3,\ ...\}$ é um subconjunto não vazio em $\mathbb{N}_0^n$ que não possui elemento mínimo, e então $>$ não é uma boa ordenação.

■

Esse lema será usado para mostrar que o algoritmo da divisão para polinômios de duas variáveis termina, pois alguns de seus termos são estritamente decrescentes (com respeito a uma determinada ordem fixada) em cada passo do algoritmo. Como um exemplo simples de uma ordem de monômios, vemos que a ordem numérica usual:

$$... > m+1 > m > ... > 3 > 2 > 1 > 0$$

nos elementos de $\mathbb{N}_0$ satisfaz as três condições da Definição 3.2. Então, a ordenação grau sobre monômios em $K[x]$ é uma ordem de monômios.

Nosso primeiro exemplo de uma ordem sobre n-uplas será a ordem lexicográfica (ou ordem lex, abreviadamente).

Definição 3.4. (Ordem Lexicográfica) Sejam $\alpha = (\alpha_1,\ ..., \alpha_n)$, $\beta = (\beta_1,\ ..., \beta_n) \in \mathbb{N}_0^n$. Dizemos que $\alpha >_{lex} \beta$ se no vetor diferença $\alpha - \beta \in \mathbb{Z}^n$ a primeira entrada não nula a partir da esquerda é positiva. Escrevemos $x^\alpha >_{lex} x^\beta$ se $\alpha >_{lex} \beta$

Exemplo 3.5. i. $(2,\ 4,\ -9) >_{lex} (1,\ 5,\ 3)$ já que $\alpha - \beta = (1,\ -1,\ -12)$

ii. $\left(-7,\ \sqrt{2},\ -6\right) >_{lex} \left(-7,\ \sqrt{2},\ -8\right)$ já que $\alpha - \beta = (0,\ 0,\ 2)$

iii. As variáveis $x_1,\ x_2,\ ...,\ x_n$ de uma equação linear, são ordenadas de maneira usual pela ordem lex, pois:

$$x_1 = x^{(1,0,...,0)},\ x_2 = x^{(0,1,0,...,0)}, ...\ x_n = x^{(0,0,...,1)}$$

e como

$$(1,0,...,0) >_{lex} (0,1,0,...,0) >_{lex} ... >_{lex} (0,0,...,1)$$

temos que

$$x_1 >_{lex} x_2 >_{lex} ... >_{lex} x_n$$

A *ordem Lex* é análoga a ordem de palavras usadas em dicionários (por isso o nome). Assim podemos ter em vista as entradas das n-uplas $\alpha \in \mathbb{N}_0^n$ de modo análogo ao das letras numa palavra, que são ordenadas alfabeticamente por $a > b > ... > y > z$. É importante dar-se conta que existem várias ordens lex, dependendo de como as variáveis são ordenadas. Até agora, temos usado a ordem lex com $x_1 > x_2 > ... > x_n$. Mas dada alguma ordem das variáveis $x_1,\ x_2,\ ...,\ x_n$, existe uma ordem lex correspondente. Por exemplo, se as variáveis são x e y , temos então uma primeira ordem lex com $x > y$ e uma segunda com $y > x$. No caso geral de n variáveis, existem $n!$ ordens lex. No que segue, a frase "ordem lex" sempre se refere para a primeira com $x_1 > x_2 > ... > x_n$, a menos que explicitada de outra forma. E na prática, quando trabalhamos com polinômios em duas ou três variáveis, chamamos as variáveis de x , y e z ao invés de x_1, x_2 e x_3.

Observe que na ordem lex, independentemente do grau total, uma variável é maior que qualquer monômio envolvendo variáveis menores, por exemplo, utilizando a ordem lex com $x > y > z$, temos $x >_{lex} y^2z^8$. Para alguns propósitos, podemos querer levar em consideração também o grau total dos monômios e ordenar monômios de maior grau primeiro. Nossa primeira forma de se fazer isso, é a *ordem lexicográfica graduada* (ou *ordem grlex*).

Definição 3.6. (Ordem Lexicográfica Graduada ou Ordem Grau-lex) Sejam $\alpha,\ \beta \in \mathbb{N}_0^n$. Dizemos que $\alpha >_{grlex} \beta$ se

$$|\alpha| = \sum_{i=0}^{n} \alpha_i > |\beta| = \sum_{i=0}^{n} \beta_i$$

ou

$$|\alpha| = |\beta| \text{ e } \alpha >_{lex} \beta$$

Assim temos que, a ordem grlex primeiro ordena pelo grau total e, caso os monômios possuam o mesmo grau total, "desempata" pela ordem lex.

Exemplo 3.7. i. $(1,1,2) > grlex\,(3,0,0)$ já que $|(1,1,2)| = 4 > 3 = |(3,0,0)|$

ii. $(2,3,5) > grlex\,(0,4,6)$ já que $|(2,3,5)| = |(0,4,6)|$ e $(2,3,5) > lex\,(0,4,6)$

iii. As variáveis são ordenadas de acordo com a ordem lex pois

$$|(1,0,...,0)| = |(0,1,0,...,0)| = ... = |(0,0,...,1)| = 1$$

Como no caso da ordem lex, existem $n!$ ordens grlex sobre n variáveis, dependendo de como as variáveis são ordenadas.

Outra ordem (um pouco menos intuitiva) em monômios é a *ordem lexicográfica graduada reversa* (ou *ordem grevlex*). Mesmo que esta ordenação "demore algum tempo para que nos acostume-mos", foi recentemente demostrado que para algumas operações, a ordem grevlex é a mais eficiente para os cálculos computacionais.

Definição 3.8. (Ordem Lexicográfica Graduada Reversa ou Ordem Grau-lex Reversa). Sejam α, $\beta \in \mathbb{N}_0^n$. Dizemos que $\alpha >_{grevlex} \beta$ se

$$|\alpha| = \sum_{i=0}^{n} \alpha_i > |\beta| = \sum_{i=0}^{n} \beta_i$$

ou

$|\alpha| = |\beta|$ e primeira entrada diferente de zero à direita de $\alpha - \beta \in \mathbb{Z}^n$ for negativa

Como grlex, a ordem grevlex ordena por grau total, mas "desempata" de uma forma diferente. Por exemplo:

Exemplo 3.9. .

i. $(5,1,3) >_{grevlex} (3,2,1)$, uma vez que $|(5,1,3)| = 9 > 6 = |(3,2,1)|$.

ii. $(0,5,2) >_{grevlex} (2,1,4)$, uma vez que $|(0,5,2)| = |(2,1,4)|$ e $(0,5,2) - (2,1,4) = (-2,3,-2)$

Note também que o lex e grevlex fornecem a mesma ordem para as variáveis de uma equação linear. Isto é,

$$(1,0,...,0) >_{grevlex} (0,1,...,0) >_{grevlex} ... >_{grevlex} (0,...,0,1)$$

ou

$$x_1 >_{grevlex} x_2 >_{grevlex} ... >_{grevlex} x_n$$

Assim, grevlex é realmente diferente de grlex na organização da ordem das variáveis.

Para mostrar a relação entre grlex e grevlex, note que tanto uma como a outra usam o grau total da mesma maneira. Em caso de empate, grlex usa ordem lex, de modo que se olha para a esquerda (ou maior) variável favorecendo a maior potência. Em contraste

o grevlex, quando encontra mesmo grau total, ele olha para a variável mais à direita (ou menor) e favorece a menor potência.

Assim, se $p = \sum_\alpha a_\alpha x^\alpha$ é um polinômio em $K[x_1, ...x_n]$ então dada uma ordem monomial $>$ podemos ordenar os monômios de p sem ambiguidades com respeito a $>$.

Exemplo 3.10. Seja $p = -5x^2y^3z - y^2z^3 + 6x^3z^3 + x^4 + xz^4 \in K[x, y, z]$

a) Na ordem lex, p fica ordenado em ordem decrescente da seguinte forma:

$$p = x^4 + 6x^3z^3 - 5x^2y^3z + xz^4 - y^2z^3$$

b) Na ordem grlex, temos:

$$p = 6x^3z^3 - 5x^2y^3z + xz^4 - y^2z^3 + x^4$$

c) Na ordem grevlex, temos:

$$p = -5x^2y^3z + 6x^3z^3 - y^2z^3 + xz^4 + x^4$$

Vamos usar a seguinte terminologia:

Definição 3.11. Seja $p = \sum_\alpha a_\alpha x^\alpha$ um polinômio não nulo em $K[x_1, ..., x_n]$ e $>$ uma ordem monomial.

i. O multigrau de p é:

$$multigrau(p) = max\{\alpha \in \mathbb{N}_0^n : a_\alpha \neq 0\} \text{ (o máximo é dado com respeito a } >).$$

ii. O coeficiente líder de p é:

$$CL(p) = a_{multigrau(p)} \in K.$$

iii. O monômio líder de p é:

$$ML(p) = x^{multigrau(p)}$$

iv. O termo líder de p é:

$$TL(p) = CL(p) \cdot ML(p) = a_{multigrau(p)} \cdot x^{multigrau(p)}$$

Exemplo 3.12. Seja $p = -2x^6z + 9x^5y^2z + 7y^8z^3 - z^5$ ordenado pela ordem lex. Então:

$$multigrau\,(p) = (6, 0, 1)$$
$$CL\,(p) = -2$$
$$ML\,(p) = x^6 z$$
$$TL\,(p) = -2x^6 z$$

Lema 3.13. *Sejam p, $q \in K\,[x_1,\ ...,\ x_n]$ polinômios não nulos. Então:*

i. $multigrau\,(p \cdot q) = multigrau\,(p) + multigrau\,(q)$.

ii. *Se $p+q \neq 0$, então $multigrau\,(p+q) \leq max\,\{multigrau\,(p)\,, multigrau\,(q)\}$. Se, além disso, $multigrau\,(p) \neq multigrau\,(q)$, então*

$$multigrau\,(p+q) = max\,\{multigrau\,(p)\,, multigrau\,(q)\}$$

Dem. (i.) Sejam $p = \sum_{i=1}^{n} a_i x^{\alpha_i}$ e $q = \sum_{j=1}^{m} b_j x^{\beta_j}$ polinômios em $K\,[x_1,\ ...,\ x_n]$ com a_i ,$b_j \in K$ e α_i, $\beta_j \in \mathbb{N}_0^n$, para $1 \leq i \leq n$ e $1 \leq j \leq m$. Seja $>$ uma ordenação monomial qualquer, de forma que podemos, sem perda de generalidade, supor:

$$\alpha_1 > \alpha_2 > ... > \alpha_n \text{ e } \beta_1 > \beta_2 > ... > \beta_m$$

e portanto temos que $multigrau\,(p) = \alpha_1$ e $multigrau\,(q) = \beta_1$.

Temos ainda que

$$p \cdot q = \left(\sum_{i=1}^{n} a_i x^{\alpha_i}\right) \cdot \left(\sum_{j=1}^{m} b_j x^{\beta_j}\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j x^{\alpha_i+\beta_j}$$

Queremos mostrar que $\alpha_1 + \beta_1$ é o grau de $p \cdot q$ e portanto

$$multigrau\,(p \cdot q) = multigrau\,(p) + multigrau\,(q)\,.$$

Para isto, observe que

$$\alpha_1 > \alpha_i \text{ para todo } 2 \leq i \leq n$$

e

$$\beta_1 > \beta_j \text{para todo } 2 \leq j \leq m.$$

e da definição de ordenação monomial temos

$$\alpha_1 + \beta_1 > \alpha_1 + \beta_j > \alpha_i + \beta_j \text{ para todo } 2 \leq i \leq n \text{ e } 2 \leq j \leq m.$$

Da mesma forma, temos que

$$\alpha_1 + \beta_1 > \alpha_i + \beta_1 > \alpha_i + \beta_j \text{ para todo } 2 \leq i \leq n \text{ e } 2 \leq j \leq m.$$

e portanto, temos que

$$\alpha_1 + \beta_1 > \alpha_i + \beta_j \text{ para todo } 2 \leq i \leq n \text{ e } 2 \leq j \leq m.$$

e portanto $\alpha_1 + \beta_1$ é o grau de $p \cdot q$.

(ii.) Sejam p e q como no item **(i.)** acima e tais que $p + q \neq 0$, de forma que $multigrau\,(p+q)$ está definido.

Suponhamos inicialmente que $multigrau\,(p) \neq multigrau\,(q)$. Temos então que $\alpha_1 > \alpha_i$ para $2 \leq i \leq n$ e $\beta_1 > \beta_j$ para $2 \leq j \leq m$. Como $\alpha_1 \neq \beta_1$, o $multigrau\,(p+q)$ será o maior entre os dois, ou seja,

$$multigrau\,(p+q) = max\,\{multigrau\,(p)\,,\ multigrau\,(q)\}$$

Se no entanto tivermos que $multigrau\,(p) = multigrau\,(q)$, então temos duas possibilidades:

1. $TL\,(p) = -TL\,(q)$

   Neste caso os temos líderes se cancelam, deixando apenas termos menores que $x^{\alpha_1} = x^{\beta_1}$ e temos que $multigrau\,(p+q) < \alpha_1 = \beta_1$ e portanto

   $$multigrau\,(p+q) < max\,\{multigrau\,(p)\,, multigrau\,(q)\}\,.$$

2. $TL\,(p) \neq -TL\,(q)$

   Neste caso os temos líderes não se cancelam e temos que

   $$TL\,(p+q) = (a_1 + b_1)\,x^{\alpha_1} = (a_1 + b_1)\,x^{\beta_1}$$

   e portanto

   $$multigrau\,(p+q) = \alpha_1 = \beta_1 = max\,\{multigrau\,(p)\,,\ multigrau\,(q)\}\,.$$

■

3.2 Algoritmo da Divisão em $K[x, y]$

Nesta seção vamos apresentar o algoritmo de divisão para polinômios em $K[x, y]$ que estende o conhecido algoritmo para $K[x]$. Nosso objetivo é dividir $p \in K[x, y]$ por $d \in K[x, y]$ com resto "pequeno", ou seja, expressar p na forma:

$$p = q \cdot d + r$$

onde o quociente q e o resto r estão em $K[x, y]$. Alguns cuidados serão necessários para caracterizar o resto e usaremos as ordens de monômios introduzidas. O caso geral, $(K[x_1, x_2, ..., x_n])$ segue de maneira análoga.

A ideia básica do algoritmo é a mesma do caso de uma variável: queremos cancelar o termo líder de p (com respeito a ordem de monômios escolhida) pela multiplicação de d por um monômio apropriado e subtraí-lo de p.

Teorema 3.14. *(Algoritmo da divisão em em $K[x, y]$). Fixamos uma ordem monomial $>$ sobre $\mathbb{N}_0^2$ e seja $d \in K[x, y]$. Então todo p em $K[x, y]$ pode ser escrita como:*

$$p = q \cdot d + r$$

onde q, $r \in K[x, y]$, e $r = 0$ ou r é uma combinação linear de monômios, com coeficientes em K, onde nenhum é divisível por $TL(d)$. Vamos chamar r de resto da divisão de p por d. Além disso, se $q \cdot d \neq 0$, então temos

$$multigrau(p) \geq multigrau(q \cdot d).$$

Dem. Vamos provar a existência de q e r e além disso fornecer um algoritmo para determiná-los.

Sejam p e $q \in K[x, y]$.

Tomemos $f_1 = p$, $q_1 = 0$ e $r_1 = 0$

i. Se $TL(d)$ divide $TL(f_1)$ então

$$q_2 = q_1 + TL(f_1) \backslash TL(d)$$

$$f_2 = f_1 - (TL(f_1) \backslash TL(d))\, d = f_1 - q_2 \cdot d$$

$$r_2 = r_1.$$

Caso contrário, temos que:

$$r_2 = r_1 + TL\,(f_1)$$

$$f_2 = f_1 - TL\,(f_1)$$

$$q_2 = q_1$$

Após ocorrer o item **(i.)** temos que $p = q_2 \cdot d + f_2 + r_2$. Continuando

ii. Se $TL\,(d)$ divide (f_2) então

$$q_3 = q_2 + TL(f_2) \backslash TL\,(d_1)$$

$$f_3 = f_2 - (TL\,(f_2) \backslash TL\,(d))\,d = f_2 - q_3 \cdot d$$

$$r_3 = r_2.$$

Caso contrário, temos que:

$$r_3 = r_2 + TL\,(f_2)$$

$$f_3 = f_1 - TL\,(f_2)$$

$$q_3 = q_2$$

Após ocorrer o item **(ii.)** temos que $p = q_3 \cdot d + f_3 + r_3$.

Esse procedimento deve ser repetido enquanto $f_i \neq 0$. Quando $f_i = 0$ temos que:

$$q = q_i \text{ e } r = r_i$$

Note que f_i representa o dividendo intermediário a cada etapa, r_i representa o resto intermediário a cada etapa e q_i é o quociente. Verificaremos que a cada vez que realizamos os itens **i.**, **ii.**, **iii.**, etc., precisamente uma das duas etapas acontecem:

Etapa da Divisão: Se $TL\,(d)$ divide f_i, então o algoritmo procede como no caso de uma variável.

Etapa do Resto: Se $TL\,(d)$ não divide f_i, então o algoritmo adiciona o $TL\,(f_i)$ para o resto.

Para provar que o algoritmo funciona, vamos primeiro mostrar que:

$$p = q \cdot d + f + r$$

é valida a cada etapa. Isto é claramente válido para os valores inicias de q, fe r. Agora suponha que a igualdade $p = q \cdot d + f + r$ é valida em cada etapa do algoritmo. Se a

próxima etapa é a **Etapa da Divisão**, então $TL(d)$ divide $TL(f)$, e a igualdade

$$q \cdot d + f = [q + TL(f)/TL(d)]\, d + (f - [TL(f)\, TL(d)]\, d)$$

mostra que a $q \cdot d + f$ não se modifica. Desde que todas as outras variáveis não são afetadas, a igualdade $p = q \cdot d + f + r$ continua verdadeira neste caso. Mas se na próxima etapa, for a **Etapa do Resto**, então f e r serão alterados, mas a soma $f + r$ é inalterada, pois:

$$f + r = [f - TL(f)] + [r + TL(f)].$$

Como antes, a igualdade $p = q \cdot d + f + r$ continua inalterada. Em seguida, note que o algoritmo termina quando $f = 0$. Nesta situação a igualdade $p = q \cdot d + f + r$ torna-se

$$p = q \cdot d + r$$

Desde que os termos são adicionados à r somente quando eles não são divisíveis por $TL(d)$, segue que q e r tem as propriedades requeridas quando o algoritmo termina.

Finalmente, precisamos mostrar que o algoritmo termina. Observe que a cada vez que redefinimos a variável *f*, ou seu multigrau diminui ou se torna 0. Para ver isto, primeiro suponha que durante a **Etapa da Divisão**, f é redefinido como

$$f' = f - \frac{TL(f)}{TL(d)} d$$

Pelo Lema 3.13, temos

$$TL\left(\frac{TL(f)}{TL(d)} d\right) = \frac{TL(f)}{TL(d)} TL(d) = TL(f)$$

então f e $(TL(f)/TL(d))\, d$ tem o mesmo termo líder. Daí, a diferença f' deve ter multigrau estritamente menor quando $f' \neq 0$. Em seguida, suponha que durante a **Etapa do Resto**, f é redefinido como

$$f' = f - TL(f)$$

Então, é obvio que $multigrau(f') < multigrau(f)$ quando $f' \neq 0$. Deste modo, em ambos os casos, o multigrau diminui. Se o algoritmo nunca terminasse, teríamos uma sequência decrescente infinita de multigraus. A Propriedade da Boa Ordenação de $>$, como vista no Lema 3.3, mostra que isto não pode ocorrer. Assim, $f = 0$ deve acontecer após um número finito de etapas.

Vamos verificar a relação entre $multigrau(f)$ e $multigrau(q \cdot d)$. Todo termo q é da forma $TL(f)/TL(d)$ para algum valor de *f*. O algoritmo começa com $f = p$, e acabamos

de provar que o multigrau de f decresce a cada etapa. Isto mostra que $TL(f) \leq TL(p)$, e então,usando a condição **(ii.)** da definição de ordem monomial, que $multigrau(q \cdot d) \leq TL(f)$ quando $q \cdot d \neq 0$. Isto completa a demonstração do teorema.

■

Exemplo 3.15. Vamos dividir $p = x^3 - 5x^2y^2 + 2xy^3 - xy$ por $d = x^2 + xy$ usando a ordem lex com $x > y$.

$$\begin{array}{rl|l} f_1 = & x^3 - 5x^2y^2 + 2xy^3 - xy & d = x^2 + xy \end{array}$$

Considere $f_1 = p$, o termo líder $TL(d) = x^2$ que divide $TL(f_1) = x^3$. Dividindo x^3 por x^2 , temos x e então subtraímos $x \cdot d$ de f_1.

$$\begin{array}{rl|l} f_1 = & x^3 - 5x^2y^2 + 2xy^3 - xy & d = x^2 + xy \\ & -x^3 - x^2y & q = x \\ \hline f_2 = & 0 - 5x^2y^2 - x^2y + 2xy^3 - xy & \end{array}$$

Agora repetimos o mesmo processo sobre $f_2 = -5x^2y^2 - x^2y + 2xy^3 - xy$. Como o termo líder $TL(d) = x^2$ divide $TL(f_2) = -5x^2y^2$, obtemos:

$$\begin{array}{rl|l} f_1 = & x^3 - 5x^2y^2 + 2xy^3 - xy & d = x^2 + xy \\ & -x^3 - x^2y & q = x - 5y^2 \\ \hline f_2 = & 0 - 5x^2y^2 - x^2y + 2xy^3 - xy & \\ & 5x^2y^2 + 5xy^3 & \\ \hline f_3 = & 0 - x^2y + 7xy^3 - xy & \end{array}$$

Novamente repetimos o mesmo processo, agora sobre $f_3 = -x^2y + 7xy^3 - xy$. Como o termo líder $TL(d) = x^2$ divide $TL(f_3) = -x^2y$, obtemos:

$$\begin{array}{rrl|l} & f_1 = & x^3 - 5x^2y^2 + 2xy^3 - xy & d = x^2 + xy \\ & & -x^3 - x^2y & q = x - 5y^2 - y \\ \hline & f_2 = & 0 - 5x^2y^2 - x^2y + 2xy^3 - xy & \\ & & 5x^2y^2 + 5xy^3 & \\ \hline & f_3 = & 0 - x^2y + 7xy^3 - xy & \\ & & x^2y + xy^2 & \\ \hline r = 7xy^3 + xy^2 - xy \quad \longleftarrow & f_4 = & 0 + 7xy^3 + xy^2 - xy & \\ \hline & f_5 = & 0 & \end{array}$$

Como o termo líder $TL(d) = x^2$ não divide nenhum dos monômios de f_4 o resto é $r = 7xy^3 + xy^2 - xy$ e concluímos a divisão. Então, temos escrito $p = x^3 - 5x^2y^2 + 2xy^3 - xy$

na forma:

$$x^3 - 5x^2y^2 + 2xy^3 - xy = \left(x^2 + xy\right) \cdot \left(x - 5y^2 - y\right) + 7xy^3 + xy^2 - xy$$

Exemplo 3.16. Neste exemplo, encontraremos uma inesperada sutileza que pode ocorrer quando trabalhamos com polinômios de duas ou mais variáveis. Vamos dividir $p = -5x^2y^2 + 2xy^3 + x^3 - xy$ por $d = x^2 + xy$ usando a ordem lex graduada com $x > y$. Note que $TL\,(d) = x^2$ divide $TL\,(p) = -5x^2y^2$. Dividindo $-5x^2y^2$ por x^2 , temos $-5y^2$ e então subtraímos $-5y^2 \cdot d$ de f_1.

$$\begin{array}{rc|l} f_1 = & -5x^2y^2 + 2xy^3 + x^3 - xy & d = x^2 + xy \\ \hline & 5x^2y^2 + 5xy^3 & q = -5y^2 \\ \hline f_2 = & 0 + 7xy^3 + x^3 - xy & \end{array}$$

Note que $TL\,(d) = x^2$ não divide $TL\,(f_2) = 7xy^3$. Entretanto, a divisão ainda ocorre, pois $TL\,(d)$ divide $x^3 - xy$. Deste modo, nós movemos $7xy^3$ para o resto e assim podemos continuar dividindo. Para implementar essa ideia, criaremos uma coluna para o resto r, a esquerda dos dividendos, onde colocaremos os termos pertencentes ao resto. Além disso, os polinômios abaixo do dividendo, serão chamados de dividendo intermediário, e continuaremos dividindo até que ele se anule.

$$\begin{array}{rrc|l} \text{r} & & f_1 = & -5x^2y^2 + 2xy^3 + x^3 - xy & d = x^2 + xy \\ \hline & & & 5x^2y^2 + 5xy^3 & q = -5y^2 + x - y \\ \hline & & f_2 = & 0 + 7xy^3 + x^3 - xy & \\ \hline 7xy^3 & \leftarrow & f_3 = & x^3 - xy & \\ & & & -x^3 - x^2y & \\ \hline & & f_4 = & 0 - x^2y - xy & \\ & & & x^2y + xy^2 & \\ \hline xy^2 - xy & \leftarrow & f_5 = & xy^2 - xy & \\ \hline r = 7xy^3 + xy^2 - xy & \leftarrow & f_6 = & 0 & \end{array}$$

Assim, o resto é $7xy^3 + xy^2 - xy$, e obtemos

$$-5x^2y^2 + 2xy^3 + x^3 - xy = \left(-5y^2 + x - y\right) \cdot \left(x^2 + xy\right) + 7xy^3 + xy^2 - xy$$

Exemplo 3.17. Agora vamos dividir $p = -5x^2y^2 + 2xy^3 + x^3 - xy$ por $d = x^2 + xy$ usando: **(i.)** a ordem lex e **(ii.)** ordem lex graduada com $y > x$.

i. Note que agora $TL\,(d) = xy$ e ele divide $TL\,(p) = 2xy^3$. As etapas da divisão seguem abaixo:

$$
\begin{array}{rrl|l}
 & f_1 = & 2xy^3 - 5x^2y^2 - xy + x^3 & d = xy + x^2 \\
 & & -2xy^3 - 2x^2y^2 & q = 2y^2 - 7xy + 7x^2 - 1 \\
\hline
 & f_2 = & 0 - 7x^2y^2 - xy + x^3 & \\
 & & 7x^2y^2 + 7x^3y & \\
\hline
 & f_3 = & 0 + 7x^3y - xy + x^3 & \\
 & & -7x^3y - 7x^4 & \\
\hline
 & f_4 = & 0 - xy - 7x^4 + x^3 & \\
 & & xy + x^2 & \\
\hline
r = -7x^4 + x^3 + x^2 \quad \longleftarrow & f_5 = & 0 - 7x^4 + x^3 + x^2 & \\
\hline
 & f_6 = & 0 &
\end{array}
$$

Desse modo temos que

$$2xy^3 - 5x^2y^2 + x^3 - xy = \left(xy + x^2\right) \cdot \left(2y^2 - 7xy + 7x^2 - 1\right) - 7x^4 + x^3 + x^2$$

ii. Nesse caso, $TL\,(d) = xy$ e ele divide $TL\,(p) = 2xy^3$. As etapas da divisão seguem abaixo:

r

$$
\begin{array}{rrl|l}
 & f_1 = & 2xy^3 - 5x^2y^2 - xy + x^3 & d = xy + x^2 \\
 & & -2xy^3 - 2x^2y^2 & q = 2y^2 - 7xy + 7x^2 - 1 \\
\hline
 & f_2 = & 0 - 7x^2y^2 - xy + x^3 & \\
 & & 7x^2y^2 + 7x^3y & \\
\hline
 & f_3 = & 0 + 7x^3y - xy + x^3 & \\
 & & -7x^3y - 7x^4 & \\
\hline
 & f_4 = & 0 - xy - 7x^4 + x^3 & \\
 & & xy + x^2 & \\
\hline
r = -7x^4 + x^3 + x^2 \quad \longleftarrow & f_5 = & -7x^4 + x^3 + x^2 & \\
\hline
 & f_6 = & 0 &
\end{array}
$$

Desse modo temos que

$$2xy^3 - 5x^2y^2 - xy + x^3 = \left(xy + x^2\right) \cdot \left(2y^2 - 7xy + 7x^2 - 1\right) - 7x^4 + x^3 + x^2$$

3.3 Fatoração Única em $K\,[x, y]$

Para finalizar este capítulo, mostraremos que todo polinômios de $K\,[x, y]$ pode ser fatorado em produto de polinômios irredutíveis.

Definição 3.18. Seja K um corpo. Um polinômio $p \in K\,[x, y]$ é irredutível sobre K se p não é constante e não é o produto de dois polinômios não constantes em $K\,[x, y]$.

Esta definição diz que se um polinômio p não constante é irredutível sobre K, então, a menos de um produto por constante, o seu único fator não constante é ele próprio. Observe também que o conceito de irredutibilidade depende do corpo.

Proposição 3.19. *Todo polinômio não constante $p \in K[x, y]$ pode ser escrito como um produto de polinômios irredutíveis sobre K.*

Dem. Se p é um polinômio irredutível sobre K, então não há nada a provar. Caso contrário, podemos escrever $p = g \cdot h$, onde g, $h \in K[x, y]$ são polinômios não constante. Note que os graus totais de g e h são menores do que o grau total de p. Agora se g ou h não for irredutível sobre K, podemos fatorá-lo em fatores não constantes. Uma vez que o grau total diminui cada vez que fatoramos, este processo pode ser repetido mais um número finito de vezes. Assim, p deve ser um produto de polinômios irredutíveis.

■

Lema 3.20. *Seja $f \in k[x]$, irredutível, tal que f divide $g \cdot h \in k[x, y]$ então $f|g$ ou $f|h$.*

Dem. Sejam $g = \sum_{i=0}^{l} a_i y_i^i$ e $h = \sum_{i=0}^{m} b_i y_i^i$, onde a_i, $b_j \in K[x]$. Se f divide cada a_i, então f divide g, e analogamente para h. Suponha, por absurdo, que f não divide g e não divide h, então existem i, $j \geq 0$ tais que $f \nmid a_i$ e $f \nmid b_j$. Vamos supor sem perda de generalidade que i e j são os menores índices com essa propriedade. Considere

$$c_{i+j} = (a_0 b_{j+i} + a_1 b_{i+j} + ... + a_{i-1} b_{j+1}) + a_i b_j + (a_{i+1} b_{j-1} + ... + a_{i+j} b_0),$$

onde c_{i+j} é o coeficiente de y^{i+j} em $g \cdot h$. Do modo que escolhemos i, f divide cada termo dentro do primeiro parênteses e, pela escolha de j, o mesmo é verdadeiro para o segundo parênteses. Mas $f \nmid a_i$ e $f \nmid b_j$, e uma vez que f é irredutível, segue da Proposição 2.28 que $f \nmid a_i \cdot b_j$, logo f não dividi c_{i+j}, e, portanto, f não divide $g \cdot h$, contradição.

■

Teorema 3.21. *Seja $f \in K[x, y]$, irredutível, tal que $f|g \cdot h \in K[x, y]$ então $f|g$ ou $f|h$.*

Dem. Suponha que f divide $g \cdot h$. Se f for um polinômio em uma variável, o resultado segue do Lema anterior. Então vamos assumir que $f \in K[x, y] \setminus (K[x] \cup K[y])$. Iremos utilizar o anel $K(x)[y]$, que é um anel de polinômio na variável y sobre o corpo $K(x)$, onde os elementos de $K(x)$ são da forma $p(x) \setminus q(x)$, onde $p(x)$, $q(x) \in K[x]$, $q(x) \neq 0$. Note que $K[x, y]$ está contido em $K(x)[y]$.

Afirmamos ainda que f é irredutível quando considerado como elemento de $K(x)[y]$. Para ver esse resultado, suponha que $f = A \cdot B$ onde A, $B \in K(x)[y]$, uma fatoração de f no anel $K(x)[y]$. Para provar que f é irredutível em $K(x)[y]$, temos de mostrar que $A \in K[x]$ ou $A \in K[x]$. Seja $d \in K[x]$ o produto de todos os denominadores de A e B. Então, $A' = d \cdot A$ e $B' = d \cdot B$ pertencem a $k[x, y]$, e

$$d^2 \cdot f = A' \cdot B' \tag{3.1}$$

em $k[x, y]$.

Pela Proposição 2.28, podemos escrever d^2 como um produto de fatores irredutíveis em $K[x]$, e, pelo Lema 3.20, cada uma delas divide *A'* ou *B'*. Podemos cancelar esse elemento em ambos os membros de (3.1), e depois de se ter anulado todos os fatores comuns, ficamos com

$$f = A'_1 \cdot B'_1$$

em $k[x, y]$.

Como f é irredutível em $k[x, y]$, implica que A'_1 ou B'_1 é constante. Como estes polinômios foram obtidos a partir de A e B, multiplicando e dividindo por vários elementos de $k[x]$, temos que $A \in K(x)$ e $B \in K(x)$.

Portanto f é irredutível em $K(x)[y]$. Disto, e do Lema 3.20, segue que $f|g$ ou $f|h$ em $K(x)[y]$

Digamos que $g = A \cdot f$ para algum $A \in K(x)[y]$. Se cancelarmos os denominadores, podemos escrever

$$d \cdot g = A' \cdot f, \tag{3.2}$$

onde $d \in K[x]$ e $A' \in K[x, y]$. Pelo lema 3.20, cada fator irredutível de d divide *A'* ou *f*. Como f é irredutível e $f \in K[x, y] \setminus (K[x] \cup K[y])$ segue que $d \nmid f$, logo $d|A'$. Mas cada vez que um fator irredutível divide *A'*, podemos cancelá-lo em ambos os membros em (3.2). Assim quando todos o cancelamentos forem feitos, vemos que f divide g em $K[x, y]$. Isso prova o teorema.

■

Teorema 3.22. *Todo polinômio não constante $f \in K[x, y]$ pode ser escrito como um produto $f = f_1 \cdot f_2 \cdot \ldots \cdot f_r$, polinômios irredutíveis sobre K e, se $f = g_1 \cdot g_2 \cdot \ldots \cdot g_s$ for outra fatoração em polinômios irredutíveis sobre K, então $r = s$ e essa expressão é única a menos da multiplicação por uma constante u e da ordem dos polinômios f_1, f_2, ..., f_r*

Dem. Pela proposição 3.19 todo polinômio não constante $p \in K[x, y]$ pode ser escrito como um produto de polinômios irredutíveis sobre K.

Agora vamos demonstrar a unicidade usando indução.

Suponhamos

$$f = u \cdot f_1 \cdot ... \cdot f_r = u' \cdot g_1 \cdot ... \cdot g_s$$

onde $u, u' \in K - \{0\}$ e $f_1,\ ...,\ f_r,\ g_1,\ ...,\ g_s$ são polinômios irredutíveis em $K[x, y]$.

Se $r = 1$, então $s = r$ já que por hipótese f_1 é irredutível.

Vamos admitir ser verdade para $r - 1$. Então

$$u \cdot f_1 \cdot ... \cdot f_r = u' \cdot g_1 \cdot ... \cdot g_s \tag{3.3}$$

implica que cada f_i divide algum g_j. Sem perda de generalidade vamos supor que $f_r | g_s$, o que implica que existe $k \in K$ tal que $g_s = k \cdot f_r$. Simplificando $k \cdot f_r$ em ambos os membros da equação 3.3, temos que

$$\tilde{u} \cdot f_1 \cdot ... \cdot f_{r-1} = u' \cdot g_1 \cdot ... \cdot g_{s-1}$$

onde $\tilde{u} = \frac{u'}{k} \in K$.

Assim, pela hipótese de indução, $r - 1 = s - 1$ e portanto, $r = s$, e segue o resultado.

■

Definição 3.23. Sejam $f,\ g \in K[x, y]$. O polinômio $d \in K[x, y]$ é chamado de *máximo divisor comum* de f e g, e denotado por $d = MDC(f, g)$, caso:

i. d divide f e g.

ii. Se d' é um polinômio qualquer que divide f e g, então d' divide d.

Vamos mostrar que $MDC(f, g)$ existe e é único a menos de uma multiplicação por uma constante diferente de zero em K. Infelizmente, o método utilizado em polinômios de uma variável para encontrar o MDC (isto é, o algoritmo de Euclides) não se estende para o caso de duas variáveis. Para ver isto, considere $f = x^2 - y^2$ e $g = x^3 + x^2 y$ polinômios em $K[x, y]$. Claramente $d = x + y$ é o $MDC(f, g)$, porém se tentarmos encontrá-lo usando o algoritmo de Euclides vamos obter outro polinômio, pois

$$x^3 + x^2 y = (x + y) \cdot \left(x^2 - y^2\right) + xy^2 + y^3,$$

e

$$\left(xy^2 + y^3\right) \nmid \left(x^2 - y^3\right)$$

nas ordens lexicográfica, lexicográfica graduada e lexicográfica graduada reversa com $x > y$.

Como resultado, nenhum polinômio se "Reduz" em relação ao outro, e não há passo seguinte para o qual se aplica o algoritmo da divisão. Portanto, pelo método de uma variável, $x^2 - y^3$ seria o MDC.

Definição 3.24. Um polinômio $m \in K[x, y]$ é chamado de *mínimo múltiplo comum* de $f, g \in K[x, y]$ e denotado $m = MMC(f, g)$ se

i. $f|m$ e $g|m$.

ii. $f|m'$ e $g|m'$, então $m|m'$.

Exemplo 3.25. $MMC\left(x^2y^2 + xy^2, x^3y + x^2y\right) = x^3y^2 + x^2y^2$.

Teorema 3.26. *Dados $f, g \in K[x, y]$, então o $MDC(f, g)$ e o $MMC(f, g)$ existem e são únicos a menos de uma multiplicação por uma constante diferente de zero em K.*

Dem. Para provar esse resultado vamos usar a fatoração única. Sejam $f, g \in K[x, y]$, tais que:

$$f = \prod_{i=1}^{n} p_i^{\alpha_i} \text{ e } g = \prod_{i=1}^{n} p_i^{\beta_i}$$

Primeiramente vamos mostrar a existência de $MDC(f, g)$. Para isso considere $d \in K[x, y]$, tal que:

$$d = \prod_{i=1}^{n} p_i^{\gamma_i}$$

onde $\gamma_i = min\{\alpha_i, \beta_i\}$. Vamos mostrar que $d = MDC(f, g)$.

Primeiro vamos mostrar que $d|f$ e $d|g$. De fato, pois se $\gamma_i = min\{\alpha_i, \beta_i\}$ então $p_i^{\gamma_i}|p_i^{\alpha_i}$ e $p_i^{\gamma_i}|p_i^{\beta_i}$ para todo i, logo $d|f$ e $d|g$.

Agora suponha $d' \in K[x, y]$, tal que $d'|f$ e $d'|g$. Então

$$d' = \prod_{i=1}^{n} p_i^{r_i}$$

onde $r_i \leq \alpha_i,\ r_i \leq \beta_i$, para todo i= 1,..., n logo

$$r_i \leq min\{\alpha_i, \beta_i\} = \gamma_i$$

e portanto $p^{r_i}|p^{\gamma_i}$, para todo $i = 1,..., n$. Logo $d'|d$ e assim concluímos que $d = MDC(f, g)$.

Agora vamos mostrar a existência de $MMC\,[f, g]$. Para isso considere $m \in K\,[x, y]$, tal que:

$$m = \prod_{i=1}^{n} p_i^{\delta_i}$$

onde $\delta_i = max\,\{\alpha_i, \beta_i\}$. Vamos mostrar que $m = MMC\,[f, g]$.

Vamos começar mostrando que $f|m$ e $g|m$. Isso é fato pois se $\delta_i = max\,\{\alpha_i, \beta_i\}$ então $p^{\beta_1}|p^{\delta_i}$ e $p^{\alpha_i}|p^{\delta_1}$ logo $f|m$ e $g|m$.

Por outro lado, para $m' \in K\,[x, y]$, se $f|m'$ e $g|m'$, então

$$m' = \prod_{i=1}^{n} p_i^{\theta_i}$$

onde $\theta_i \geq \alpha_i,$ e $\theta_i \geq \beta_i,$ para todo $i = 1,..., n$, logo

$p^{\delta_1}|\theta_i$, para todo $i = 1,..., n,$ o que implica que $\theta_i \geq max\,\{\alpha_i, \beta_i\}\,,$ para todo $i= 1,..., n$

portanto $m|m'$ e $m = MDC\,(a, b)$.

A unicidade dos dois resultados segue da fatoração única.

■

Exemplo 3.27. Sejam $f = x^2y^3+x^2y^2+2xy^2+2xy+y+1$ e $g = xy^3+2xy^2+xy+y^2+2y+1$ polinômios em $K\,[x, y]$. Como:

$$f = x^2y^3 + x^2y^2 + 2xy^2 + 2xy + y + 1 = (xy + 1)^2\,(y + 1)$$

e

$$g = xy^3 + 2xy^2 + xy + y^2 + 2y + 1 = (xy + 1)\,(y + 1)^2$$

então,

$$d = MDC\,(f, g) = (xy + 1)\,(y + 1) = xy^2 + xy + y + 1$$

e

$$m = MMC\,[f, g] = (xy + 1)^2\,(y + 1)^2 = x^2y^4+2x^2y^3+x^2y^2+2xy^3+4xy^2+2xy+y^2+2y+1$$

Referências

[1] Hefez, A., **Elementos de Aritmética**, $2^{a.}$ Edição, Rio de Janeiro, SBM, 2011.

[2] Gonçalves, A., **Introdução à Álgebra**, $5^{a.}$ Edição, Rio de Janeiro, IMPA, 2012.

[3] Garcia, A. e Lequain, Y., **Elementos de Álgebra**, $5^{a.}$ Edição, Rio de Janeiro, IMPA, 2010.

[4] Boyer, C. B., **História da Matemática / Carl B. Boyer; Revista por Uta C.Merzbach; Tradução Elza F. Gomide**, $2^{a.}$ Edição, São Paulo, Edgard Blücher, 2003.

[5] Milies, C. P., **Uma Breve História da Álgebra Abstrata**, Notas de Aula, São Paulo, IME. URL ⟨ http://www.bienasbm.ufba.br/M18.pdf⟩.

[6] Marques, A. D., **O Estudo de Pesos Generalizados de Hamming Através de Equações Polinomiais**, Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG, 2010

[7] Cox, D., Little, J., O'Shea, D., **Ideals, Varieties, and Algorithms**, $3^{a.}$ Edição, Springer, 2006.

[8] Buchberger, E. von B., **Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem Nulldimensionalen Polynomideal**, Dissertação de Doutorado, Universitat Innsbruck-Austria, 1965.

[9] Santos, J. P. de O., **Introdução à Teoria dos Números**, $3^{a.}$ Edição, Rio de Janeiro, IMPA, 2010.